(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 196 20 137 A1**

(51) Int. Cl.[6]:
H 04 L 29/06
H 04 L 12/52
H 04 L 1/12
H 04 B 17/00
H 04 B 7/212
H 04 B 7/26

(21) Aktenzeichen: 196 20 137.3
(22) Anmeldetag: 7. 5. 96
(43) Offenlegungstag: 13. 11. 97

DE 196 20 137 A1

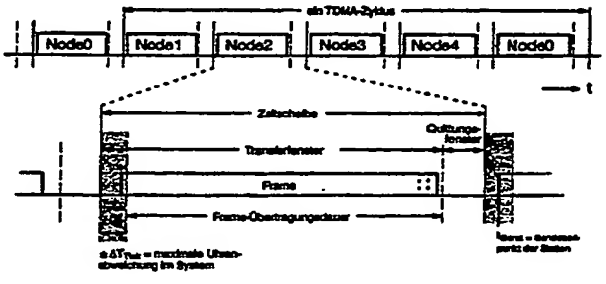
(71) Anmelder:
Daimler-Benz Aktiengesellschaft, 70567 Stuttgart, DE

(72) Erfinder:
Bohne, Jürgen, Dipl.-Ing., 10555 Berlin, DE

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Protokoll für sicherheitskritische Anwendungen

(57) Es soll ein Protokoll zur Übertragung von Nachrichten zwischen sendenden und empfangenden Stationen in Zeitscheiben für sicherheitskritische Anwendungen auf der Basis einer synchronen Arbitration angegeben werden, durch das insbesondere auch bei redundanten Stationen Störungen im Kommunikationssystem (einschließlich der Kommunikationsteilnehmer) zuverlässig ermittelt werden. Dazu werden die Zeitscheiben zyklisch jeweils einer Empfangsstation durchgängig deterministisch zugeordnet. Die Zeitscheiben werden jeweils in ein zeitliches Transferfenster zur Übertragung der Nachricht bzw. einer Teilnachricht und in ein an das Transferfenster anschließendes zeitliches Quittungsfenster unterteilt, wobei im Quittungsfenster ausschließlich bei einer fehlerhaft oder gar nicht empfangenen Nachricht von der Empfangsstation ein Einspruchsignal (VETO-Signal) als Anzeige einer Störung abgegeben wird.



DE 196 20 137 A1

Beschreibung

Kommunikationssysteme arbeiten oft in einer Umgebung, deren Störpotential nicht genau definiert werden kann. Dies gilt vor allem für Automotive-Anwendungen, deren Störumgebung sich ständig ändert. Verkehrsmittel, wie z. B. Kraftfahrzeuge, sind besonders gefährdet beim Durchqueren starker Felder in der Nähe von Sendern und durch Gewitter, die starke burst-artige Störungen produzieren. Im Pkw und Nfz werden heute bereits elektronische Steuerungskomponenten eingesetzt, die untereinander Daten austauschen bzw. gemeinsame Datenquellen nutzen. Die verwendeten Kommunikationssysteme [1] erfüllen die daran geknüpften Zuverlässigkeitsanforderungen:

- Kommunikationsfehler müssen entdeckbar sein.
- Der Ausfall eines Teilnehmers darf das Kommunikationssystem nicht lahmlegen.
- Die Reihenfolge der Nachrichten eines Senders bleibt beim Empfang erhalten.
- Nachrichten werden mit hoher Wahrscheinlichkeit rechtzeitig übertragen.

Zur Zeit werden die ersten Kfz-Komponenten entwickelt und erprobt, die sicherheitskritische Aufgaben bewältigen und dazu miteinander kommunizieren. Gegenstand der Forschung sind Komponenten, die gemeinsam sicherheitskritische Aufgaben unter harten Echtzeitbedingungen erfüllen, so daß das Kommunikationssystem selbst sicherheitskritisch ist. Solche Anwendungen stellen erweiterte Anforderungen an das Kommunikationssystem, die von den derzeitigen Systemen nur teilweise erfüllt werden:

- Das Kommunikationssystem muß fail-operational sein, d. h. es muß bei jeder möglichen Störung und nach jedem möglichen Ausfall seine Aufgabe weiter erfüllen (u. U. müssen redundante Kommunikationswege unterstützt werden).
- Das Kommunikationssystem muß permanente Fehler von Störeinstreuungen zuverlässig unterscheiden und defekte Komponenten — und nur solche — vom Senden ausschließen.
- Änderungen im Kommunikationssystem (Ausfall und Wiederanlauf) müssen der Anwendung schnellst möglich und netzweit konsistent gemeldet werden.
- In den Nachrichten müssen Verfälschungen bis hin zur maximal vorkommenden Länge einer Störung (Burst) zuverlässig erkannt werden.
- Wichtige Nachrichten sind in garantierter Zeit zu übertragen.
- Multicast-Nachrichten sind erforderlich und müssen atomar übertragen werden. Für bestimmte Nachrichten von verschiedenen Quellen ist die Erhaltung ihrer globalen Reihenfolge zu garantieren.
- Es muß ein Sicherheitsnachweis führbar sein, worin ausgeschlossen wird, daß das Kommunikationssystem Sicherheitsfunktionen in den einzelnen Komponenten beeinträchtigen kann. Wenn Komponenten gemeinsam eine sicherheitskritische Aufgabe bearbeiten, muß ein Sicherheitsnachweis für das Kommunikationssystem unter Einschluß aller Komponenten geführt werden.

Neben den Zuverlässigkeits- und Sicherheitsanforderungen stellt die Praxis weitere Anforderungen an ein Kommunikationssystem:

- Dynamisches Aus- und Eingliedern von Kommunikationsteilnehmern und Erweiterbarkeit des Netzes sind wichtige Eigenschaften. Als Beispiel sei folgende Idee genannt:
  Zur Ankopplung eines modernen Anhängers an ein modernes Nfz wird die Station, die das Ankoppeln eines allen Anhängers ermöglicht, für die Fahrt ausgegliedert. Die Stationen im modernen Anhänger werden angeschlossen und eingegliedert.
- Eine weitere wichtige Eigenschaften ist die leichte Integrierbarkeit von Stationen und Funktionen in ein und zu einem Gesamtsystem, da bereits die Ausstattungsvarianten eines Pkws die unterschiedlichsten Zusammenstellungen von Funktionen erfordern. Die einzelnen Stationen müssen dabei leicht konfigurierbar sein.
- Ein zukunftsorientiertes Kommunikationssystem muß mit der Entwicklung Schritt halten und weiterentwickelt werden können. Es sollte für höhere Übertragungsgeschwindigkeiten geeignet und auf verschiedenen physikalischen Medien lauffähig sein. Denkbare Anwendungsarchitekturen, insbesondere für den redundanten Betrieb, dürfen nicht behindert oder gar verhindert werden.
- Und: Das Kommunikationssystem muß kostengünstig sein.

Kommunikationsprotokoll

"Motor" eines Kommunikationssystems ist sein Protokoll. Dieser Bericht stellt ein Protokoll vor, das im Gegensatz zu den asynchronen Protokollen CAN [2] und ABUS [3] im Kfz-Bereich oder TCN [4] im Bahnbereich einen Ansatz auf Basis einer synchronen Arbitration vorsieht. Das Protokoll berücksichtigt die vorgenannten Anforderungen, ist äußerst robust gegen Störungen und ergreift alle Möglichkeiten, um die Kommunikation aufrecht zu erhalten. Es setzt eine synchrone verteilte Zeitbasis voraus, die über die laufenden Nachrichten [5] und durch lokale Uhren [6] realisiert werden kann. Ein TDMA-Ansatz, wie er im SAFEbus [7] zu finden ist, der für sichere Systeme in der Luftfahrt als Backplane-Bus (42 Inches) konzipiert wurde, ist für das lokale Netz im Kfz zu aufwendig.

Das Protokoll präjudiziert keine bestimmte Software-Architektur für die Anwendung. Es ist offen für Kombinationen aus einfachen Stationen, die einen Kommunikationsweg nutzen, bis hin zu hochredundanten Stationen,

die redundante Kommunikationswege nutzen. Neben dem Leitmotiv Fehlertoleranz und Sicherheit werden bei der Entwicklung des Protokolls Aspekte wie Praktikabilität, Kosten und Weiterentwicklung in hohem Maße berücksichtigt.

Zeitgesteuerte Architektur

Für sicherheitskritische Systeme ist das statische (Pre-Runtime) Scheduling von Anwendungsprozessen wegen der leichteren Verifizierbarkeit von Vorteil. Ein naheliegender Gedanke besteht in der Synchronisation von Protokoll und Anwendung, wodurch eine zeitgesteuerte Architektur entsteht. In einer Time Triggered Architecture (TTA) steuert ein globaler Zeittakt, der verteilt realisiert sein kann, alle Systemaktivitäten: Anwenderfunktionen und Kommunikation. Der Informationsfluß in einer solchen Architektur kann wie folgt ablaufen: Eine Nachricht wird in einer vorbestimmten Zeitscheibe produziert, in der nachfolgenden Zeitscheibe gesendet und empfangen und während der nächsten Zeitscheibe in der Empfängerstation weiterverarbeitet (Delivery-Delay minimal, Delivery-Jitter = 0). Das vorliegende Protokoll und das Time Triggered Protocol TTP [8], das ebenfalls für Anwendungen im Kfz vorgesehen ist, kann Teil einer solchen durchgängig zeitgesteuerten Architektur sein.

Durchgängig zeitgesteuerte Architekturen und ihre statischen Aktivitätszuteilungen besitzen große Vorteile, besonders im Hinblick auf redundante Stationen. Sie weisen jedoch auch ein paar Probleme auf:

— Wenn z. B. beim Transport Nachrichten gestört werden oder verloren gehen, bleibt für eine erneute Übertragung keine Zeit. TTP sieht in solchen Fällen konsequent die Ausgliederung betroffen er Stationen vor.
— Da jede Komponente in ihrem Zeitverhalten auf das Gesamtsystem abgestimmt sein muß, werden Kosten und Aufwand zum Problem, wenn eine zeitgesteuerte Architektur auf ein variantenreiches System bzw. Produkt angewandt wird und nicht auf ein Spezialprodukt. Es wird sowohl für unterschiedliche Fahrzeugtypen als auch für verschiedene Ausstattungsvarianten verschiedene Konfigurationen der gleichen Komponente geben. Das macht ein Konfigurationsmanagement beim Bau eines Kfz und beim nachträglichen Einbau und Austausch von Komponenten erforderlich.
— In der Luft- und Raumfahrt werden zeitgesteuerte Systeme eingesetzt, die beim Wechsel von Flugphasen sogenannte Mode Changes durchführen. Verschiedene Modi, also unterschiedliche Vergabe von Senderechten, sind in zeitgesteuerten Systemen notwendig, wenn ein System an eine veränderte Situation angepaßt werden muß. Mode Changes sind deshalb auch in TTP und PROSA vorgesehen. Die Durchführung eines Mode Change bereitet jedoch im Störungsfall unter Konsistenz- und Realzeitgesichtspunkten große Probleme, auch wenn die Modi starken Beschränkungen unterworfen werden und nicht beliebige Modi gestattet sind. Sie können deshalb nur im störungsfreien Fall durchgeführt werden. Zudem muß jeder Modus von jeder Komponente, auch wenn sie selbst keine unterschiedlichen Modi benötigt, mitgetragen werden. Das bedeutet, jede Komponente muß prinzipiell in jedem Modus ihre Aufgabe erfüllen. Die internen zeitlichen Abläufe müssen mit den Modi konform gehen.

Fazit

Das Protokoll sollte keine generelle Synchronisation mit der Anwendung erzwingen, sollte sie jedoch ermöglichen, so daß Teile der Anwendung gleichzeitig zeitgesteuert, zeitgesteuert-protokollsynchron und ereignisgesteuert arbeiten können.

Eine zeitgesteuerte, auch protokollsynchrone Software-Architektur kann für ein sicheres und hochverfügbares Kfz-Grundsystem, das z. B. aus einer redundanten Fahrerstation und vier Radmodulstationen besteht, sinnvoll sein. Alle anderen Teile, wie z. B. die Stationen des Beleuchtungssystems, können ereignisgesteuert arbeiten.

Mode Changes, also Sprünge in unterschiedliche Zeitscheibenvergaben während des Betriebs, sollten nach Möglichkeit vermieden werden und nicht zum normalen Ablauf gehören.

Das erfindungsgemäße Protokoll, also das Protokoll für sicherheitskritische Anwendungen, wird im folgenden auch abgekürzt als PROSA bezeichnet.

1. Vorgaben, Randbedingungen

Das Protokoll arbeitet funktional unabhängig von der Anwendung und kann von letzterer in seinem Ablauf nicht beeinflußt werden. Es stellt jeder Station ein gewisses Maß an Übertragungskapazität pro Zeiteinheit zur Verfügung. Solange die dort lokalisierte Anwendung innerhalb dieser Grenzen Transferleistungen an fordert, kann eine maximale Übertragungszeit unter gegebenen Störbedingungen garantiert werden. Eine spezielle Konfiguration des Protokolls ist wegen der Unabhängigkeit von der Anwendung nicht notwendig. Die Koordination der verschiedenen Zulieferer von Stationsmodulen bezüglich des Protokolls ist minimal und beschränkt sich auf die Verwendung einer abgestimmten, eindeutigen Stationsadresse und u. U. Subadresse.

Protokoll-Typ

Das Protokoll basiert auf dem TDMA-Arbitrationsverfahren: Time Division Multiple Access. Beim TDMA-Verfahren wird die Zeit in Zeitscheiben unterteilt, die in allen Stationen weitgehend synchron gehalten werden. Jeder Station ist in einem TDMA-Zyklus eine eigene Zeitscheibe statisch zugeordnet. Innerhalb ihrer Zeitscheibe hält die Station das ausschließliche Senderecht auf dem gemeinsamen Kommunikationsmedium. Dieses

Verfahren ist effizient, wenn, wie in unserem Fall, die Anzahl der Kommunikationsteilnehmer und die Nachrichtenlängen eher gering sind. Beide Parameter sind, neben der Übertragungsrate der Hardware, die wirtschaftlich vertretbar sein muß, die bestimmenden Faktoren für die Zugriffszeit.

Ein großer Vorteil von TDMA ist der deterministische Zugriff. Eine totale Blockade des Kommunikationssystems ist prinzipbedingt ausgeschlossen. Im fehlerfreien Fall kann jeder Station eine maximale Zeitdauer für die Übertragung ihrer Nachrichten garantiert werden, wenn sie die ihr zugestandene Kapazitätsgrenze beachtet. Um auch bei Störungen und Ausfällen eine Maximalzeitdauer beim Nachrichtentransport zu gewährleisten, muß das einfache TDMA-Verfahren zum Protokoll erweitert werden.

Andere synchrone Protokolle, wie das Token-Bus-Protokoll [9] und seine Varianten, haben, im Gegensatz zum TDMA-Protokoll, im Fehlerfall eine veränderte Zugriffszeit (Probleme: Tokenverlust und -generierung) oder sie stellen, wie das Token-Ring-Protokoll [10], die schwer zu erfüllende Forderung nach einer aktiven Kommunikationsstrecke.

Störungen

Je höher die Übertragungsgeschwindigkeit auf einer Kommunikationsleitung ist, desto eher werden Störungen wirksam. Die möglichen Störungen, denen ein Kfz ausgesetzt ist und die die Einrichtungen im Kfz selbst produzieren, müssen entweder konstruktiv oder vom Protokoll beherrscht werden. Da sind zunächst stochastische, auch burst-artige Störungen, die von außen eingestreut werden, oder die von internen Schaltvorgängen stammen. Zum anderen gibt es auch interne oder vom Nachbarn kommende periodische Störungen, die sich auf den Ablauf eines periodischen Protokolls besonders ungünstig auswirken können. Dies sind beispielsweise Störungen durch Zündung und Generator, deren Periode sich außerdem in Abhängigkeit von der Drehzahl ändert. Wenn solche Störungen auch nur zeitweilig durchschlagen — und dies kann z. B. auch durch Produktionsfehler, Alterungsfehler oder durch Wartungsfehler an den Entstörbauteilen geschehen — kann eine bestimmte Drehzahl auf ein streng periodisch es TDMA-Protokoll eine fatale Wirkung haben.

Beispiele

Mögliche Störquelle Zündung: 4 Zylinder, 5000 U/min
→ Zündperiode: ≈ 6 ms
→ Zündimpuls: ≈ 150 µs
versus TDMA-Protokoll: Datenrate 1 MBit/s, 32 Teilnehmer, 3 + 16 Byte Frame-Länge
→ Zykluszeit: ≈ 6 ms
→ Übertragungsdauer der Nachricht: ≈ 150 µs

Das bedeutet, die Zündung kann eine bestimmte Zeitscheibe im Zyklus eines simplen TDMA-Protokolls periodisch so stören, daß die zugehörende Station zwangsläufig ausgegliedert wird, weil ein permanenter Fehler angenommen werden muß. Da die Perioden von Protokoll und Zündung niemals exakt gleich sind, kann danach auch die nächste Station ausgegliedert werden.

Mögliche Störquelle Generator:
Halbwellen bis 10 KHz = 100 µs-Periode (18 000 U/min: 12-polig = 300 µs/16-polig = 200 µs)
Solche schnell-periodischen Störungen müssen konstruktiv so weit unterdrückt werden, daß sie nicht dauerhaft, sondern allenfalls statistisch wirksam werden, da sie anderenfalls in jeder TDMA-Zeitscheibe auftreten und deshalb wie eine permanente Störung wirken.

Festlegung der Randbedingungen

— Topologie des Kommunikationssystems:
Es wird ein bitserieller Bus — z. B. Koax- oder (abgeschirmte) Zweidrahtleitung — verwendet, dessen maximale Länge in etwa 100 m beträgt und der redundant vorhanden sein kann. An die Busleitung sind die Teilnehmerstationen mittels Transceiver so angeschlossen, daß eine Blockade des Nachrichtenverkehrs durch permanenten Hardware-Fehler einer einzelnen Station ausgeschlossen ist.

— Anforderungen an die Kommunikationsteilnehmer:
Die Teilnehmerstationen besitzen eine Fehlervermeidungseinrichtung, die sicherstellt, daß ein Sendeversuch außerhalb der stationseigenen Zeitintervalle abgefangen wird. Stationen sind weiterhin in der Lage, spezielle Signale (VETO) zu erzeugen, die auch unter starken Störeinflüssen mit sehr hoher Wahrscheinlichkeit erkannt werden. Die Signale haben eine so spezielle Ausprägung, daß es nur selten dazu kommt, daß eine Störung als VETO-Signal interpretiert wird. VETO-Signale müssen außer ihrer Anwesenheit keine weitere Information übermitteln.

— Länge der Nachrichten, Nachrichten pro Zeiteinheit:
Die benötigte Nachrichtenlänge der Anwendungen liegt voraussichtlich zwischen einigen Bytes und einigen zehn Bytes. Sollen auch zukünftige datenintensive Anwendungen, z. B. Streckenführung, über dieses Kommunikationssystem betrieben werden, wäre der Einsatz einer Hochgeschwindigkeits-Hardware unumgänglich.

— Anzahl der Kommunikationsteilnehmer:
Die aktuelle Anzahl der Teilnehmerstationen kann variieren. Die maximale Anzahl der Stationen, die Realzeit-Transportbedingungen fordern, kann bei den voraussichtlich erforderlichen Zugriffszeiten (unter 10 ms), den vorgenannten Nutzdatenmengen und den heute gebräuchlichen Übertragungsgeschwindigkeiten (1 bis 10 MBit/s) bei etwa 32 liegen. Wird Hardware mit größerer Übertragungsgeschwindigkeit

eingesetzt, kann die maximale Anzahl der Stationen erhöht werden.
— Qualität des Nachrichtentransports (Verlust, Verdopplung, Reihenfolge, Transportdauer):
Das Anforderungsspektrum an die Kommunikation ist sehr breit. Anwendungen im Fahrzeug benötigen je nach Aufgabe
— sehr schnellen Buszugriff mit Übertragungsgarantie, z. B. Bremssystem,
— häufigen, eventuell periodischen Buszugriff, z. B. Motorsensorik,
— oder seltenen Zugriff mit geringen Zeitanforderungen, z. B. Fenstersteuerung.
Das Protokoll muß also einerseits wichtige Nachrichten auch im Störungsfall schnell mit Zeitgarantie transportieren, andererseits darf es unwichtige Nachrichten vernachlässigen.
— Verbindungsart (synchron, asynchron), Kommunikationsbeziehungen (1 zu 1,1 zu n):
Nachrichten sollen aus Gründen der Konsistenz und Erweiterbarkeit des Systems broadcast gesendet werden, was eine verbindungsorientierte Arbeitsweise ausschließt. Die Protokollmaschine arbeitet unabhängig von der Anwendung, d. h. Anwendernachrichten werden entweder einzeln wartend (synchron) oder über Warteschlangen (asynchron) übergeben und nach Möglichkeit versendet. Liegt keine Nachricht vor, handelt die Protokollmaschine nach eigenen Notwendigkeiten.
— Art und Häufigkeit von Störungen aus der Umgebung:
Das Protokoll soll in stark gestörten Umgebungen mit häufigen, auch periodisch auftretenden Übertragungsfehlern, die mitunter burst-artig andauern können, zuverlässig arbeiten. Es soll permanente Fehler der Kommunikations-Hardware erkennen und den betroffenen Teilnehmer ausgliedern. Transiente Störungen sollen nicht zur Ausgliederung einer Station führen. Eine Station muß sich in das laufende Protokoll eingliedern können.
— Zulässige Störungen durch das Kommunikationssystem in die Umgebung:
Bei Verwendung gekapselter Stationen und abgeschirmter Busleitungen können Störungen durch die Kommunikation in die Umgebung, sowie Störungen aus der Umgebung, stark reduziert werden. Das Protokoll ergreift hierzu keine Maßnahmen.

2. Protokoll

Aus Gründen der besseren Verständlichkeit des Protokolls wurde in diesem Ideenpapier eine informelle Beschreibungsform gewählt; eine OSI-konforme Beschreibung des Protokolls kann bei Bedarf erstellt werden. Das folgende Kapitel enthält eine Kurzeinführung in das Protokoll. Eine detaillierte Beschreibung, Protokollzustände und Regeln, sind in den anschließenden Kapiteln dargelegt.

2.1 Grundzüge des Protokolls

Das TDMA-Arbitrationsverfahren wird unter der Philosophie Silence is Consent zum Kommunikationsprotokoll erweitert. Dazu werden die Zeitscheiben jeder Station in zwei Zeitintervalle, ein Transferfenster und ein kurzes nachfolgendes Quittungsfenster, unterteilt. Wird im Quittungsfenster "geschwiegen", gilt die vorangegangene Sendung als akzeptiert.
Bild 1 zeigt die in ein Transferfenster und in ein Quittungsfenster unterteilten Zeitfenster als Prinzipbild im ungestörten Betrieb.

Quittungsfenster kein Manko

Bei oberflächlicher Betrachtung wird durch die Einführung des Quittungsfensters, auch wenn es nur wenige Bitübertragungszeiten dauert, Übertragungskapazität verschenkt. Dabei ist jedoch zu bedenken, daß jede reale Protokollmaschine (Protocol Controller) nach Empfang eines Frames eine gewisse Zeit benötigt, um die Nachricht zu überprüfen, an die Anwendung zu übergeben und die eigene, nachfolgende Sendung zu präparieren. Es wird also, auch wenn einige Funktionen parallelisierbar sind, eine Pause zwischen zwei Frames geben. Protokollkontrolle, Übergabe und Präparation können bei geschickter Planung der Protokollmaschine während des Quittungsfensters durchgeführt werden.
Ein Vorteil des Quittungsfensters ist seine Lage zwischen den Sendefenstern, die es nicht zuläßt, daß Störungen, die kürzer einwirken, als das Quittungsfenster breit ist, zwei aufeinander folgende Nachrichten-Frames zerstören. Deshalb sollte das Quittungsfenster mindestens so breit sein wie die Dauer der häufiger vorkommenden Störungen.

Ablauf bei Störungen

In Umkehrung bedeutet Silence is Consent: Wenn eine Station eine Störung entdeckt, legt sie im Quittungsfenster Einspruch in Form eines VETO-Signals ein. Im Fall, daß die sendende Station oder eine Station, die ein Nachrichten-Frame korrekt empfangen hat, VETO erkennt — es kann sich in seltenen Fällen auch um eine Störeinstreuung handeln, die als VETO interpretiert wird — sendet sie ebenfalls VETO. Diese Festlegung wird getroffen, um die Wahrscheinlichkeit, daß alle Stationen VETO erkennen, zu erhöhen, sie dient auch der Sicherstellung der Konsistenz im System bei redundantem Bus mit einkanaligen Stationen. Das Senden von VETO-Signalen wird kurz vor Erreichen der neuen Zeitscheibe eingestellt.
Nach einer Störung wird ein Rekonfigurationszyklus durchlaufen. Er dient der Ermittlung der Fehlerursache und ggf. der Lokalisation und Ausgliederung einer defekten Station. Im Zyklus werden spezielle Rekonfigurations-Frames gesendet (im Bild grau unterlegt), die jedoch ebenfalls Anwendernachrichten enthalten. Inkorrek-

ter Empfang im Zyklus wird ebenfalls durch VETO markiert. Handelt es sich um einen Fehler des Senders (**Bild 2**) oder um eine Störung, die noch während des Zyklus abklingt (**Bild 2** und 3), werden die in den Frames enthaltenen Anwendernachrichten weitergeleitet.

In **Bild 2** ist eine Einzelstörung dargestellt.

Bild 3 zeigt demgegenüber eine anhaltende Störung.

Zum Abschluß des Rekonfigurationszyklus wird der normale Betrieb wieder aufgenommen. Spätestens nach der erneuten Sendung in der initial gestörten Zeitscheibe (**Bild 4**: Zeitscheibe des Node 0) würde auch die Ausgliederung einer ausgefallenen Station oder einer Station mit permanentem Fehler im Sende- oder Empfangskanal geschehen. Jede Station führt dazu lokal einen Systemzustandsvektor, in dem sie laufend den aktuellen Zustand der Partnerstationen einträgt. Diese Information (membership service) steht auch der Anwendung jederzeit konsistent zur Verfügung.

Bild 4 zeigt den Ausfall einer Station bzw. einen permanenten Sendefehler.

2.2 Zeitscheibenvergabe, Zykluswechsel (Mode-Change)

In einem TDMA-Zyklus besitzt jede Station, die Nachrichten versendet, mindestens eine Zeitscheibe, in der sie sendeberechtigt ist. Da nicht alle Stationen gleichberechtigt behandelt werden müssen, kann — unter Wahrung der vorgenannten Aussage — eine problemangepaßte Zeitscheibenvergabe im TDMA-Zyklus gewählt werden. So können redundante Stationen oder Stationen, die kürzere Zugriffszeiten benötigen bzw. größere Informationsmengen zu übertragen haben, zwei oder mehr Zeitscheiben im TDMA-Zyklus besitzen. Als Beispiel sei eine Zeitscheibenvergabe vorgestellt, die ein Kfz-Grundsystem (0 Fahrerstation, 1..4 Radmodule) bevorzugt und Rechenzeit nach der Kommunikation vorsieht, in der andere Stationen (5, 6, 7, 8) senden:

... 4 8 1 0 5 1 2 3 4 6 0 7 1 2 3 4 8 1 0 5 ...

Die Zeitscheibenvergabe muß jedoch global und konsistent im Kommunikationssystem bekannt sein. Sie wird im folgenden als statisch vorgegeben angenommen. Führt man den Gedanken der Anpassung der Kommunikation weiter, kommt man zu dem Wunsch mehrere unterschiedliche TDMA-Zyklen im System zur Verfügung zu haben. Damit gelangt man zum Problem des Zykluswechsels oder Mode-Change. Läßt man Mode-Changes zu, sollte man sich darüber im Klaren sein, daß ein Time-Guardian — das ist eine von der Protokollmaschine unabhängige Hardware-Einrichtung, die sicherstellt, daß Sendeversuche außerhalb der stations-eigenen Zeitintervalle abgefangen werden — notwendigerweise komplexer wird.

Zykluswechsel in PROSA werden auf Anforderung der Applikation einer Station wirksam, wenn der neue Zyklus bei allen anderen aktiven Stationen von ihrer Applikations-Software freigegeben wurde und sie deshalb kein VETO eingelegen. Der neue TDMA-Zyklus beginnt mit der angeforderten Zeitscheibe.

2.3 Redundante Kommunikations-Hardware

Wenn die Protokollmaschine von vornherein zwei Eingangskanäle besitzt, kann bei Bedarf ein zweiter Transceiver angeschlossen werden, der eine zweite Busleitung ankoppelt. Im Fall eines permanenten Fehlers eines Transceivers oder einer Busleitung kann bei redundanter Auslegung die Kommunikation aufrecht erhalten werden und das Kfz bleibt fahrfähig. Sind alle Teile in Ordnung, ist die Wahrscheinlichkeit für die Wirksamkeit einer Übertragungsstörung herabgesetzt. Dies ist zwar begrüßenswert, für das Protokoll jedoch von geringerem Einfluß, da auch mit einer Leitung und einem funktionsfähigen Transceiver der Betrieb bei auftretenden Störungen unbedingt sichergestellt sein muß. Dies ist besonders kritisch, wenn trotz Warnung (zur Werkstatt) weitergefahren wird. Festlegung:

1. Eine Station sendet im Normalfall auf beiden Kanälen zeitgleich Nachrichten-Frames und ggf. VETO-Signale. Die Übertragung eines Frames gilt zunächst als erfolgreich, wenn eine Station mindestens eines der redundanten Frames, egal von welcher Leitung, korrekt empfängt. Wird nachfolgend auf einer der beiden Leitungen VETO erkannt — eine andere Station hatte keinen korrekten Empfang — gilt die Übertragung als gescheitert.
2. Der gleichzeitige Betrieb von Stationen, die beide Leitungen eines redundanten Busses betreiben, und solchen, die (ausfallbedingt) nur eine Leitung betreiben, ist zulässig.

2.4 Frame-Format (Rahmen-Format)

Anwendernachrichten werden in Frames "eingerahmt" versendet. Unter Verwendung eines selbsttaktenden Codes bei der physikalischen Übertragung kann Bit-Stuffing im Frame unterbleiben, wenn ein Endekenner des Frames unnötig ist. Bei variablen Nachrichtenlängen hat man die Wahl, die Endekennung durch Interframe-Spacing (Ruhe auf der Leitung) sicherzustellen oder am Anfang des Frames eine Längenangabe mitzusenden, die dann aber die Empfangs-Hardware auswerten muß. Damit ist jedoch, wie beim Bit-Stuffing, der Nutzinformationsanteil verringert. Auch die Tatsache, daß die Länge aller Nachrichten zur Compile-Zeit eines Gesamtsystems bekannt ist, kann von der Protokollmaschine genutzt werden, indem sie diese Längenangaben zur Initialisierungszeit einliest.

Bei variabler Frame-Länge hat man in jedem Fall den Nachteil, daß sowohl die Protokollmaschine als auch der bereits erwähnte Time-Guardian komplexer werden. Die einfachste Methode, die zunächst im Prototyp verwen-

det werden soll, besteht darin, Frames konstanter Länge zu senden, wodurch auch alle Zeitscheiben die gleiche Länge aufweisen.

Frames bestehen aus folgenden Feldern:

Preamble/Startdelimiter:
Dient zur Synchronisation der Empfänger.

F Frame type (1 Bit):
Normal-Frame, Recovery-Frame

E1, E2 Error flags (2 Bit) im Recovery-Frame:
gesetzt, wenn ein Empfangsfehler auf dem assoziierten Bus aufgetreten ist

C Cycle number (1 Bit) im Normal-Frame:
Alle aktiven Stationen übermitteln über das C-Bit in den Normal-Frames aufeinander folgender Zeitscheiben die Nummer des aktuellen TDMA-Zyklus (Mode). Eine Sequenz besteht aus einer Reihe von Normal-Frames mit gesetztem C-Bit, die von Normal-Frames mit gelöschtem C-Bit begrenzt werden. Die Summe der Frames mit gesetztem C-Bit ergibt die Nummer des Zyklus. Beispiel:

$$\text{C-Bit}(\text{N-Frame}_{\text{slice}})_{\text{slice}=n,n+1,n+2\ldots}:\{\ldots010\ldots\} \triangleq \text{Zyklus 1}$$

Die Kenntnis der aktuellen Zyklusnummer ist notwendig, wenn sich eine neu anlaufende Station in den laufenden Protokollbetrieb integrieren will. Eine Störung macht die Übermittlung ungültig.

S Slice number (1 Bit) im Normal-Frame:
Eine Stationen übermittelt über das S-Bit in ihren Normal-Frames ständig die Nummer der Zeitscheibe, in der sie gerade sendet, und damit implizit — unter Kenntnis der aktuellen Zyklusnummer — auch ihre eigene Stationsadresse. Eine Sequenz besteht aus einer Reihe von Normal-Frames mit gesetztem S-Bit, die von Normal-Frames mit gelöschtem S-Bit begrenzt werden. Die Summe der Frames mit gesetztem S-Bit ergibt die Nummer der Zeitscheibe.

Beispiel

$$\text{S-Bit}(\text{N-Frame}_{\text{slice},i})_{\text{slice}=\text{const}/i=n,n+1,n+2\ldots}:\{\ldots0110\ldots\} \triangleq \text{slice 2}$$

Die Kenntnis der Zeitscheibennummer ist notwendig, wenn sich eine neu anlaufende Station in den laufenden Protokollbetrieb integrieren will und ihre eigene Zeitscheibe bestimmen muß. Eine Störung macht die Übermittlung ungültig.

M Message type (1 Bit):
Protokoll-Nachricht (Type: NULL, INIT, CHMODE, INTEGRATE..),
Applikationsnachricht
Protokollnachrichten werden während der Initialisierung, Eingliederung und im Betrieb gesendet; letzteres, wenn keine Anwendernachricht vorliegt.

R Redundant OK (1 Bit):
gesetzt als Bestätigung von der aktiven redundanten Station, wenn eine Zwillingsstation eine erfolgreiche Eingliederung versucht hat.

I Input error (1 Bit):
gesetzt, wenn einer der Eingangskanäle der Sendestation permanent defekt ist (unterstützt Systemmonitoring).

B Bus mode (1 Bit):
spiegelt den aktuellen Sendemodus der Station; wenn gesetzt sendet die Station auf beiden Bussen gleichzeitig.

Message:
Dieses Feld enthält die Anwendernachrichten, die unterschiedlich lang sein können. Bei geringer Länge können u. U. mehrere Nachrichten in einem Frame transportiert werden. Eine große Nachricht muß in mehreren Frames versendet und wieder zusammengesetzt werden. Da die Stationsnummer eines Absenders eindeutig feststeht, kann auf eine Anwendertypkennung in der Nachricht verzichtet werden, wenn ein Absender nur einen Nachrichtentyp produziert.
Im Nachrichtenfeld von Protokollnachrichten ist der Typ, die Nummer des augenblicklichen Zykluses, die Position der augenblicklichen Zeitscheibe im Zyklus, der stationsgeführte Zustandsvektor des Kommunikationssystems und eine Prüfsumme über die Zeitscheibenvergaben eingeschrieben.

CRC:
Der Cyclic Redundancy Check überdeckt das Protokoll-Byte und die Nachrichten im Frame. Er wird parallel zum Senden generiert und angefügt und parallel zum Empfang generiert und überprüft. Um eine zuverlässige Fehlererkennung zu gewährleisten, sollte der CRC mindestens eine Bit-Länge aufweisen, die der maximalen, in der Praxis vorkommenden Länge einer (schnellen Mehrfach- oder Burst-) Störung entspricht.

3. Die Protokollmaschine

Der Nachrichten-, Kommando- und Informationsaustausch von Anwender-CPU und Protokollmaschine geschieht über einen Dual Port RAM (DPR). Die Anwendung kann daher nicht in den Protokollablauf eingreifen. Das Anschlußschema der Protokollmaschine sieht im Prinzip wie in Fig. 5 dargestellt aus:
Die Protokollmaschine besitzt auf der Netzwerkseite zwei serielle Eingänge und einen Ausgang zum direkten Anschluß zweier Transceiver. Die Sendeverstärker der Transceiver werden durch zwei separate Signalleitungen ein- oder abgeschaltet. Die Protokollmaschine hat keine Kenntnis, ob tatsächlich redundante Busleitungen angeschlossen sind, arbeitet jedoch nach Voreinstellung in diesem Sinne. Ist nur ein Transceiver und Bus angeschlossen oder ein Kanal defekt, ändert das am Protokollablauf nichts, lediglich die Wahrscheinlichkeit, daß eine Störung wirksam wird, vergrößert sich. Ob eine VETO-Leitung notwendig ist oder VETO als spezielles Signal auf der Transmit-Leitung gegeben wird, hängt von der Realisierung des VETO-Signales ab; die Leitung geht — wenn vorhanden — an beide Transceiver.

3.1 Protokollschnittstelle zur Anwendung

Die Anwendungsschnittstelle ist auf die oben beschriebene Dual-Port-Ankopplung bezogen. Bei Verwendung eines anderen Schnittstellentyps sind die folgenden Ausführungen sinngemäß zu übertragen.

Startauftrag, Zustandswechsel

Die Protokollmaschine lädt direkt nach dem Einschalten ihre Zustandsvariable im DPR mit dem Wert PENDING und durchläuft dann ihre Initialisierung und ihren Selbsttest. Danach signalisiert sie SUCCESS oder FATAL_ERROR. Bei SUCCESS kann von der Anwendung der Startauftrag in die Kommandovariable geschrieben werden und die Protokollmaschine startet in die Initialisierung oder in den Passivbetrieb (nur Empfang). Vor dem Auftrag wird von der Anwendung die Stationsadresse, die Nummer des Zyklus, der nach der Initialisierung angesprungen werden soll, und die Zyklusinformation im DPR eingetragen, letztere wird durch eine Prüfsumme geschützt. Nach Abschluß ihrer Operationen informiert die Protokollmaschine die Anwendung über ihren Zustand: SUCCESS, EXCLUDED (vom Senden ausgeschlossen) oder FATAL_ERROR und stellt der Anwendung die aktuellen Protokollinformationen, wie z. B. Nummer der Zeitscheibe und Nummer des Zyklus, über den DPR bereit. Die Protokollmaschine kann jederzeit über die Kommandovariable aufgefordert werden, in den Normalbetrieb oder in den Passivbetrieb umzuschalten.

Zykluswechsel

Es existieren zwei Variablen, die den Kommandozyklus steuern. Die Variable AcceptCycle muß auf allen Stationen von der Applikation mit der Nummer des neuen Zyklus geladen werden, bevor die Applikation auf einer Station ihre Protokollmaschine durch Laden der Variablen InitCycle veranlaßt, das Gesamtsystem in den anderen Zyklus zu versetzen.

Sende-Modi

Die Protokollmaschine kann jederzeit über die Variable SendMode in einen anderen Sendemodus geschaltet werden. Zur Unterstützung der Arbeit redundanter Stationen stehen folgende Modi zur Verfügung:
SEND_NONE: nicht senden (jedoch VETO)
SEND_ANY: in jeder Zeitscheibe auf beiden Bussen senden (Voreinstellung), beim Senden wird das B-Bit im Protokollbyte gesetzt
SEND_BUS 1/2: auf Bus 1/2 senden
SEND_EVEN/ODD: in gerader/ungerader Zeitscheibe auf beiden Bussen senden
SEND_CROSSWISE1: in gerader Zeitscheibe auf Bus 1, in ungerader auf Bus 2 senden
SEND_CROSSWISE2: in gerader Zeitscheibe auf Bus 2, in ungerader auf Bus 1 senden
SEND_BUS1EVEN: in gerader Zeitscheibe auf Bus 1 senden
SEND_BUS1ODD: in ungerader Zeitscheibe auf Bus 1 senden
SEND_BUS2EVEN: in gerader Zeitscheibe auf Bus 2 senden
SEND_BUS2ODD: in ungerader Zeitscheibe auf Bus 2 senden

Sendeauftrag/Sendestatus

Die Sendeverwaltung besteht aus einer Struktur (Ring oder FIFO) mit je zwei Einträgen pro Sendung: Speicheradresse und Rückmeldevariable. Mit jedem Sendeauftrag wird die Speicheradresse der Anwendernachricht in den Sendering geschrieben. Die Rückmeldevariable wird von der Anwendung auf den Wert PENDING gesetzt.
Beim synchronen oder wartenden Sendeauftrag wird die Anwendung die Rückmeldevariable abfragen, beim asynchronen Sendeauftrag erwartet sie möglicherweise einen Interrupt, sobald eine Nachricht übertragen ist oder verworfen wird.
Folgende Rückmeldestati können vorliegen:
PENDING: Nachricht wurde noch nicht übertragen
SUCCESS: Nachricht wurde übertragen

TRANSFER_ERROR: Nachricht wurde übertragen, jedoch durch VETO invalidiert
EXCLUDED: N. nicht übertragen, weil selbst vom Senden ausgeschlossen
FATAL_ERROR: N. nicht übertragen, eigene Kommunikation permanent defekt

Empfangsauftrag/Empfangsstatus

Mit dem Empfangsauftrag wird der Protokollmaschine ein Verwaltungsvektor übergeben, der auf jeweils zwei Empfangspuffer für die Nachrichten beider Busse pro Zeitscheibe verweist, oder NULL enthält, wenn kein Empfang erwünscht ist. Der Vektor enthält außerdem die Empfangsstati jeder Zeitscheibe.

Beim synchronen Empfang wird die Anwendung den Empfangsstatus abfragen, ob eine Nachricht eingetroffen ist; beim asynchronen Empfang erwartet sie möglicherweise einen Interrupt. Der Empfangsstatus besteht aus dem Transferstatus und den 2 Protokoll-Bytes der Busse.

Der Transferstatus kann folgende Werte annehmen:
PENDING Beginn der Nachrichtenübertragung
SUCCESS: mind. eine Nachricht wurde korrekt empfangen
NO_MESSAGE: Es wurde keine Anwendernachricht gesendet
TRANSFER_ERROR: Es wurde kein Frame (korrekt) empfangen
FATAL_ERROR: eigene Kommunikation permanent defekt
Folgender Wert ist ausschließlich im Passivbetrieb möglich:
MESSAGE_ERROR: keine korrekte Nachricht erhalten, wurde global nicht invalidiert
Außerdem sind folgende Zusatzanzeigen im Status von großem Interesse:
VETO: Zeitscheibe wurde global invalidiert
SYSCHANGE: eine Station wurde vom Senden ausgeschlossen oder hat den Normalbetrieb (wieder)aufgenommen
EXCLUDED: Eigner der Zeitscheibe ist vom Senden ausgeschlossen
BUS1ERROR: Nachricht wurde auf Bus 1 nicht oder inkorrekt empfangen
BUS2ERROR: Nachricht wurde auf Bus 2 nicht oder inkorrekt empfangen

Interrupt, Interrupt-Freigabe

Voreinstellungsmäßig sind alle Ereignisse, die den Interrupt auslösen können, maskiert und müssen von der Anwendung freigegeben werden (Interrupt-Mask-Variable). Die Protokollmaschine schreibt am Ende der Zeitscheibe die Ereignisse in die Ereignisvariable und generiert einen Interrupt.

Wenn das korrespondierende Typ-Bit in der Maske gesetzt ist wird der Interrupt:
NEXTSLICE: ausgelöst, wenn die nächste Zeitscheibe beginnt
RX_READY: ausgelöst, wenn eine Nachricht eingetroffen ist
TX_READY: ausgelöst, wenn eine eigene Nachricht gesendet oder verworfen wurde
VETO: ausgelöst, wenn im Quittungsfenster einer aktiven Station invalidiert wurde (ermöglicht auch das Führen einer Fehlerstatistik)
SYSCHANGE: ausgelöst, wenn irgend eine Station vom Senden ausgeschlossen wurde oder den Normalbetrieb (wieder)aufgenommen hat oder eine Änderung im ReceiveState einer Station auftritt
EXCLUDED: ausgelöst, wenn die eigene Station vom Senden ausgeschlossen wurde
INCLUDED: ausgelöst, wenn die eigene Station eingegliedert wurde.
MODECHANGE: ausgelöst, wenn ein Zustandswechsel durchgeführt wurde
In einer zeitgesteuerten Architektur (TTA) ist nur der Interrupt NEXTSLICE von Bedeutung, mit dessen Hilfe die Anwendung mit dem Protokoll synchronisiert wird. Alle weiteren Informationen können der Ereignisvariablen entnommen werden.

Lesen des aktuellen Systemzustands

Der Systemzustandsvektor, der Zustand der eigenen Protokollmaschine, die aktuelle Zeitscheibennummer und die aktuelle Zyklusnummer können jederzeit gelesen werden. Die Variablen werden jeweils kurz vor Beginn einer neuen Zeitscheibe aktualisiert und sind mit Beginn jeder neuen Zeitscheibe (NEXTSLICE) konsistent.

3.2 Arbeitsweise der Protokollmaschine

Die Protokollmaschine arbeitet nach folgendem Zustandsdiagramm, das in Bild 6 dargestellt ist:
Nach Einschalten und auf Anforderung der Anwender-Software geht die Protokollmaschine in die Initialisierung. In der Initialisierungwerden andere Kommunikationsteilnehmer angesprochen und ein TDMA-Zyklus aufgebaut. Im Anschluß wechselt die Protokollmaschine in den Normalbetrieb oder, wenn von der Applikation gewünscht, in den Passivbetrieb. Der Passivbetrieb gestattet der Anwendung ein Mithören der Nachrichten; die Protokollmaschine ist jedoch nicht sendeberechtigt. Wenn bereits ein Zyklus von anderen Stationen aufgebaut wurde, wechselt die Protokollmaschine von der Initialisierung über den Zustand Eingliederung in den Normalbetrieb. Auch aus dem Passivbetrieb heraus kann auf Veranlassung der Anwendung über die Eingliederung der Wechsel in den Normalbetrieb erfolgen. Ein Übertragungsfehler versetzt die Protokollmaschine aus dem Normalbetrieb in den Zustand Rekonfiguration. Es wird ein Rekonfigurationszyklus durchlaufen, in dem festgestellt wird, ob ein permanenter Fehler vorliegt. Die Protokollmaschine wechselt, wenn sie von einem solchen Fehler betroffen ist, in den Passivbetrieb. Nach Fehlerstatistik und erfolgreichem Selbsttest kann eine erneute

Eingliederung versucht werden, oder sie kann abschaltet werden.

4. Festlegungen und Regeln

Die nachfolgenden Festlegungen und Regeln sind zugleich Implementierungsvorschriften für die Protokollmaschine. Sie werden teilweise durch Zeitdiagramme ergänzt, die das resultierende Verhalten des Kommunikationsgesamtsystems — bezüglich der Regeln — versinnbildlichen. Der Begriff "Station" wird synonym für "Protokollmaschine" verwandt.

Protokollgrundregeln

Regel 1

Stationen erhalten eine sie eindeutig kennzeichnende numerische Adresse "i". Stationen haben außerdem Kenntnis von allen TDMA-Zyklen (Modes), die im Betrieb vorkommen können. Jeder Zyklus besteht aus einer Reihe von Zeitscheiben, die bestimmten Stationen zugeordnet sind. In einem Zyklus können mehrere Zeitscheiben einer Station zugeordnet sein. Die Zyklen sind statisch festgelegt und allen Stationen konsistent bekannt. Eine Station "i" im aktuellen Zyklus "c" besitzt in allen Zeitscheiben der Nummer "s" mit owner(c,s) = i das Senderecht; im Fall owner(c,s) ≠ i darf sie nicht senden.

Regel 2

Eine Station besitzt normalerweise aus Redundanzgründen zwei Kommunikationskanäle (Transceiver), die mit zwei Busleitungen verbunden sind. Beim Senden werden deshalb per Voreinstellung (default) beide Sendekanäle selektiert. Davon unberührt ist jedoch der gleichzeitige Betrieb von Stationen, die real auf zwei Kanälen senden und empfangen, und solchen, die nur einen Kanal zur Verfügung haben (gewollt oder defekt), zulässig. Stationen im redundanten Betrieb selektieren nach Aufforderung durch die Anwendung beim Senden ihrer Nachrichten nur einen oder keinen Kanal, siehe Regel 38. Alle Frames einer Station reflektieren über das B-Bit des Protokollbyte ihren aktuellen Sendemodus. Diese Information ist der Empfangsseite der Anwendung zugänglich.

Regel 3

Ein Empfangsfehler liegt vor, wenn in einer Zeitscheibe von einem Empfänger kein Frame empfangen wurde oder kein Frame korrekt empfangen wurde (frame error, crc error). Bei Empfang eines korrekten Frames gilt die Übertragung als erfolgreich.

Stationen, die einen Empfangsfehler erkannt haben, senden im nachfolgenden Quittungsfenster grundsätzlich VETO. Eine Station selektiert beim Senden von VETO grundsätzlich beide Kanäle. Dadurch wird bei redundantem Anschluß auf beiden Leitungen VETO gesendet. Stationen, die nach Regel 1 in keinem Zyklus eine Zeitscheibe besitzen, sind überhaupt nicht berechtigt zu senden und dürfen auch kein VETO senden.

Regel 4

Eine Station, die im Quittungsfenster VETO erkennt, sendet ebenfalls bis zum Ende des Quittungsfensters auf beiden Kanälen VETO (auch wenn sie ein korrektes Frame empfangen hat). Dadurch wird die Konsistenz mit einkanalig defekten Stationen sichergestellt. Das Quittungsfenster ist aus diesem Grund mindestens doppelt so groß wie die Zeitdauer für das Erkennen des VETO-Signals. (Jedoch auch mindestens so groß, wie die häufiger vorkommenden Störungen).

Regel 5

Jede Station führt einen Systemzustandsvektor, in dem der Zustand aller Stationen auf dem letzten Stand gehalten wird. Stationen sind excluded oder included gesetzt.

Regel 6

Empfängt eine Station auf einem Kanal von mehr als der Hälfte der included gesetzten Stationen keine korrekten Frames, setzt sie den Kanal undefined. Es besteht der Verdacht einer Busunterbrechung oder eines Kurzschlusses. Sie setzt den Kanal ok, sobald sie (wieder) mehr als die Hälfte der Stationen auf dem Kanal korrekt empfängt.

Regel 7

Ist einer der Kanäle undefined gesetzt, werden alle eigenen Frames mit gesetztem I-Bit im Protokollbyte gesendet, so daß dies für alle Stationen sichtbar wird. Die Information wird der Anwendung über den Empfangsstatus gemeldet.

Nachrichtenregeln

Regel 8

Die Protokollmaschine holt eine Anwendernachricht, sobald ihre Zeitscheibe erreicht wird, oder sie generiert eine Protokollnachricht vom Typ NULL, wenn keine Nachricht vorliegt. Protokollnachrichten enthalten die Nummer des aktuellen Zyklus, die Position der augenblicklichen Zeitscheibe im Zyklus, den aktuellen Systemzustandsvektor und eine geeignete Prüfsumme über die Zyklen.

Regel 9

Sind in einem korrekt empfangenen Frame Anwendernachrichten enthalten, werden sie nach Ablauf des Quittungsfensters der Anwendung übergeben. Jeder Nachricht wird im Empfangsstatus ein Transferstatus mitgegeben. Der Transferstatus enthält u. a. eine Information, ob die empfangene Nachricht systemweit invalidiert oder von allen aktiven Stationen akzeptiert wurde (VETO).

4.1 Normalbetrieb

Protokollregeln

Regel 10

Im Normalbetrieb werden von allen aktiven Stationen Normal-Frames (N) in ihrem Zeitfenster gesendet. (Siehe auch Regel 8 und 9). Normalbetrieb besteht, solange alle aktiven Empfänger in den Zeitfenstern included markierter Sender (mindestens) ein Normal-Frame korrekt empfangen, wie aus Bild 7 zu ersehen ist.

Regel 11

Im Quittungsfenster einer excluded gesetzten Station wird nach Regel 3 VETO gesendet. In diesem Fall wird von allen Stationen der Normalbetrieb fortgesetzt. (Siehe auch Regel 34). Dieses ist in Bild 8 dargestellt.

Regel 12

Die included gesetzten Stationen übermitteln über das Cycle-Bit im Protokoll-Byte kontinuierlich die Nummer des augenblicklichen Zyklus. Die erste Station beginnt mit einer 0 im Cycle-Bit, die Nachfolger senden dann nacheinander so oft eine 1, bis die Nummer des Zyklus erreicht ist. Danach sendet die nächste Station wieder eine 0 usw., siehe auch Regel 20 (Gegenpart). Beim Verlassen des Normalbetrieb oder nach Senden einer Protokollnachricht wird der Mechanismus zurückgesetzt, bis er mit dem ersten ungestörten Normal-Frame (das logischerweise eine 0 im Cycle-Bit enthält) wieder einsetzt.

Regel 13

Eine Station übermittelt in ihrer(n) Zeitscheibe(n) über das Slice-Bit im Normal-Frame die Nummer der augenblicklichen Zeitscheibe (und damit implizit ihre Stationsadresse). Sie beginnt mit einer 0 im Slice-Bit und sendet danach in der gleichen Zeitscheibe so oft eine 1, bis die Nummer der Zeitscheibe erreicht ist. Danach beginnt sie von vorn. Gegenpart: Regel 21. Beim Verlassen des Normalbetrieb oder nach Senden einer Protokollnachricht wird der Mechanismus zurückgesetzt, bis er mit dem ersten ungestörten Normal-Frame der Station wieder einsetzt.

4.2 Rekonfiguration

Wenn die im Zustand Normalbetrieb gesendeten Frames eines included gesetzten Senders von mindestens einem Empfänger nur gestört oder gar nicht empfangen wurden, durchlaufen alle Stationen einen Rekonfigurationszyklus. Für eine solche Störung kommen folgende Ursachen in Betracht:

1. Störeinstreuung,
2. total ausgefallene Station,
3. Station(en) mit defektem(n) Empfangskanal(kanälen),
4. Station mit defektem Sendekanal,
5. Trennung oder Kurzschluß der Busleitung(en), die sich in Form von Station(en) mit Totalausfall und/oder in Form von Station(en) mit defektem Empfangskanal zeigt.

Die Rekonfiguration soll permanente Störursachen beseitigen, soll jedoch im Fall transienter Störungen keine Station fälschlicherweise ausgliedern. In den Fällen 1 bis 4 ist eine eindeutige Ursachenfindung möglich, das heißt die Entscheidung ob und welche Station ausgegliedert werden muß, kann eindeutig und korrekt getroffen werden. Unter den geforderten Realzeitbedingungen kann eine derart korrekte Entscheidung — wenn es eine gibt — im Fall 5 nicht garantiert werden. Es ist jedoch möglich, die Eintrittswahrscheinlichkeit für den Fall 5 durch Verwendung redundanter Busleitungen und durch Wartung gegen Null zu bringen.

Im Rekonfigurationszyklus werden ausschließlich Recovery-Frames gesendet, die in ihren Error-Flags einen Teil der Information tragen, die zur Ursachenfindung notwendig ist. Für die Rekonfiguration sind drei Stationsvariablen relevant:

— Über die Error-Flags im Recovery-Frame informiert die Station alle anderen Stationen, ob sie beide Frames des eingangs gestörten Senders inkorrekt empfangen hat.
— In der Variablen ReceiveOneOk merkt sich die Station, ob sie im Rekonfigurationszyklus mindestens ein Frame von einer anderen Stationen korrekt empfängt.
— In der Variablen OtherDisturbed merkt sich die Station, ob mindestens eine andere Station (ebenfalls) beide Frames des eingangs gestörten Senders inkorrekt empfangen hat.

Die Stationen treffen nach Ende des Rekonfigurationszyklus ihre Entscheidung. An der Entscheidung beteiligt sind die Empfänger, die das Frame des eingangs gestörten Senders, der im Anschluß an den Rekonfigurationszyklus erneut sendet, gestört empfangen haben. Von diesen gliedern sich die Stationen aus, die von keinem Sender ein korrektes Frame empfangen haben oder die als einzige von den wiederholt gestörten Frames des Senders betroffen waren. Alle anderen an der Entscheidung beteiligten Empfänger signalisieren das Aus des eingangs gestörten Senders durch Aussenden des VETO-Signals.

Regel 14

Stellt eine Station im Normalbetrieb fest, daß im Quittungsfenster einer Station VETO gesendet wurde, die im Systemzustandsvektor included gesetzt ist, führt sie nachfolgend einen Rekonfigurationszyklus durch. (Im Rekonfigurationszyklus werden grundsätzlich keine CHMODE-Nachrichten gesendet).

a1) Zu Beginn des Rekonfigurationszyklus setzen Stationen, die bei der vorangegangenen Sendung einen Übertragungsfehler festgestellt, ihre Variablen wie folgt
— beide Error-Flags im Recovery-Frame TRUE (R1),
— ReceiveOneOK = FALSE,
— OtherDisturbed = FALSE.
a2) Stationen, die mindestens ein korrektes Normal-Frame empfangen haben, setzen ihre Variablen
— mind. ein Error-Flag im Recovery-Frame FALSE (R0),
— ReceiveOneOK = TRUE,
— OtherDisturbed = TRUE.
b1) Alle included gesetzten Stationen senden im Rekonfigurationszyklus in ihrer/n Zeitscheibe/n ein Recovery-Frame mit den zuvor gesetzten Error-Flags (R0/R1). Dies gilt nicht für den eingangs gestörten Sender, wenn er mehrere Zeitscheiben im Zyklus besitzt; er sendet ein Normal-Frame (N). (Siehe auch Regel 8 und 9).
Stationen, die im Zyklus einen Übertragungsfehler bemerken, senden — wie in Regel 3 vereinbart — VETO, so daß bei der Auslieferung von Nachrichten an die Anwendung die globale Sicht gewährleistet bleibt.
b2) Bei korrektem Empfang eines Frames — egal ob durch VETO invalidiert — setzen die Empfänger ihre Variablen
— ReceiveOneOk = TRUE (ein Frame wurde korrekt empfangen) und, wenn beide Error-Flags im Recovery-Frame TRUE gesetzt sind,
— OtherDisturbed = TRUE (eine andere Station war eingangs gestört).
c) Wird im Rekonfigurationszyklus ein nach Regel 14b1 gesendetes Normal-Frame (N) des eingangs gestörte Senders nicht invalidiert, gilt unmittelbar sofort wieder Normalbetrieb.
d) Nach Ende des Rekonfigurationszyklus sendet der eingangs gestörte Sender ein Normal-Frame (N).
e) Stellt ein Empfänger nach dem Empfang des gemäß Regel 14d gesendeten Frames einen Übertragungsfehler fest, wertet er seine Variablen aus:
e1) Ist die Variable ReceiveOneOk FALSE, konnte er kein Frame korrekt empfangen.
Der Empfänger gliedert sich nach Regel 15 aus.
e2) Ist die Variable ReceiveOneOk TRUE und die Variable OtherDisturbed FALSE, war er der einzige Teilnehmer, der keine korrekten Nachrichten vom Sender bekommen hat (das erste Frames und das letzte Frame können durchaus auch bei anderen Stationen inkorrekt empfangen sein). Der Empfänger wartet das Quittungsfenster ab. Wird von anderen Stationen VETO ausgelöst, bleibt er im aktiven Betrieb; wird jedoch kein VETO ausgelöst, gliedert er sich nach Regel 15 aus.
e3) Ist die Variable ReceiveOneOk TRUE und die Variable OtherDisturbed TRUE, wird die Sendung invalidiert, wodurch der Sender nach Regel 16 ausgegliedert wird.
(s. Bild 9)

Regel 15

Ausgliederung eines Empfängers: In beiden Fällen (Regel 14e1 oder 14e2) setzt der Empfänger eine Meldung (MSGERROR/EXCLUDED/SYSCHANGE) an die Anwendung ab und geht in den Passivbetrieb.

Regel 16

Ausgliederung eines Senders: Im Fall einer Invalidierung (Regel 14e3) wird der Sender konsistent ausgeglie-

dert. Alle aktiven Stationen, auch der Sender selbst, markieren den Störenfried im Systemzustandsvektor als excluded. Die Ausgliederung des Senders wird der Anwendung bekannt gegeben (EXCLUDED/SYSCHANGE). Der Sender geht in den Passivbetrieb. In der nächsten Zeitscheibe wird der Normalbetrieb fortgesetzt.

Bild 10 zeigt den Ablauf des Protokolls bei permanent defektem Empfangskanal.

Bemerkung: Bei einer Störung, die nicht über den Rekonfigurationszyklus hinaus anhält, bleibt der betroffene Sender und alle Empfänger aktiv, siehe **Bild 9**. Hält eine Störung über den Rekonfigurationszyklus hinaus an, bleibt mindestens eine Station aktiv, entweder der Sender oder bei Teilstörungen mindestens einer der Empfänger (vgl. **Bild 11**).

Bemerkung: Regel 14c ist geeignet bei günstiger Verteilung der Stationen im Zyklus Ausgliederungen durch einfach-periodische Störungen zu vermeiden, wie das aus **Bild 12** erkennbar ist.

4.3 Initialisierung

Wenn eine Station zur Initialisierung aufgefordert wird, sind folgende Fälle zu betrachten:

— Es läuft schon ein TDMA-Zyklus:
die Station wechselt in den Zustand Eingliederung.
— Sie versucht, einen TDMA-Zyklus aufzubauen, indem sie ein erstes S1-Frame sendet. Dabei sind folgende Fälle zu unterscheiden:
  — Eine andere Station versucht auch, einen TDMA-Zyklus aufzubauen.
  — Andere Stationen antworten nicht (Übertragungsfehler, Kollision, keine Station aktiv).
  — Andere Stationen akzeptieren den Versuch.

Regel 17

Zu Beginn der Initialisierung wird von der Protokollmaschine der TDMA-Zyklus 0 erzeugt. Darin besitzt jede, in den statisch festgelegten Zyklen vorkommende Station genau eine Zeitscheibe. Die Stationen werden in aufsteigender Adreßreihenfolge eingetragen.

Der Regel 17 liegt folgendes grobes Zustandsdiagramm zugrunde, das in **Bild 13** dargestellt ist.

a) Wird eine Station von der Anwendung zur Initialisierung aufgefordert, wartet sie eine festzulegende Zeitspanne, die den gemeinsamen Start aller Stationen ermöglichen soll, auf ein Frame. Die Zeitspanne sollte so groß gewählt sein, daß die unterschiedlichen Laufzeiten bei der Initialisierung der Stationen ausgeglichen werden. Sie muß größer sein als die Zyklusdauer, um ein laufendes System nicht zu stören.

b1) Bekommt eine wartende Station in der o.g. Zeit ein korrektes Frame, das nicht vom Typ INIT-Protokollnachricht ist, wechselt sie in den Zustand Eingliederung.

b2) Wenn die Station nach Ablauf der o.g. Zeitspanne kein Frame bekommen hat, sendet sie eine eigene initiale INIT-Nachricht. Letztere enthält, wie jede Protokollnachricht die Nummer des Zyklus (= 0), die Nummer der Zeitscheibe im Zyklus (und damit implizit die Stationsadresse), den aktuellen Systemzustandsvektor und eine Prüfsumme über die Zeitscheibenvergaben. Im initialen Zustandsvektor sind die Bits aller Stationen excluded gesetzt. In der INIT-Nachricht wird das eigene Zustandsbit included gesetzt.

b3) Erhält die Station auf ihre INIT-Nachricht innerhalb einer Zeitspanne, die sich aus <Zykluszeit + 2 • Zeitscheibennummer • Zeitscheibenzeit> bestimmt, kein Frame einer anderen Station, sendet sie erneut ihre initiale INIT-Nachricht. Dieser Vorgang wird "I"-mal wiederholt ("I" muß noch festgelegt werden).

b4) Wird zu dieser Zeit ein Frame gestört empfangen, wird kein VETO gesendet und erneut nach Regel b3 verfahren. Dabei wird die o.g. Wartezeit erneut gesetzt.

b5) Nach Erhalt einer ersten korrekten INIT-Nachricht wird die enthaltene Prüfsumme mit der eigenen verglichen. Stimmen sie überein wird die Zeitscheibe mit Hilfe der enthaltenen Zeitscheibennummer synchronisiert, und die Protokolluhren (Timer) werden nach Regel 40 gestartet. Im Fall einer Differenz schaltet sich die Empfängerstation ab.

c1) Jedesmal, wenn nachfolgend eine INIT-Nachricht korrekt empfangen wird, wird die enthaltene Prüfsumme mit der eigenen verglichen. Im Fall einer Differenz wird das Frame invalidiert. Anderenfalls wird der enthaltene Systemzustandsvektor entnommen und lokal überschreibend gespeichert. Gestörte oder invalidierte Frames werden ignoriert. Nach korrektem Empfang von Frames, die nicht vom Typ INIT sind, geht das Protokoll in den Zustand Eingliederung.

c2) Gelangt eine Station, die in ihrem lokalen (zuletzt gespeicherten) Systemzustandsvektor noch excluded gekennzeichnet ist, in ihre Zeitscheibe, kopiert sie den Zustandsvektor in ihre INIT-Protokollnachricht, setzt dort ihr Zustandsbit included und sendet das Frame ab.

c3) Ist eine Station in ihrer Zeitscheibe bereits included gesetzt, sendet sie eine Protokollnachricht vom Typ CHMODE mit dem gewünschten Erstzyklus und geht, wenn nicht invalidiert wird, in den Normalbetrieb. Der Normalbetrieb beginnt mit der Zeitscheibe o des vereinbarten Zyklus (siehe auch Kapitel 4.6). Die Aufnahme des Normalbetriebs wird der Anwendung bekannt gegeben.

d) Alle Stationen, die eine Protokollnachricht vom Typ CHMODE empfangen, die nicht invalidiert wird, schalten ebenfalls in den Normalbetrieb, wenn ihr Bit im Systemzustandsvektor included gesetzt ist. Ist das nicht der Fall, gehen sie in den Zustand Eingliederung. Die Aufnahme des Normalbetriebs wird der Anwendung bekannt gegeben.

Bild 14 zeigt den normalen Start des Protokolls.

In Bild 15 ist der Start des Protokolls nach einer Kollision dargestellt.

4.4 Passivbetrieb

Die Anwendung kann die Protokollmaschine in den Passivbetrieb starten oder umschalten. Der Passivbetrieb wird automatisch aufgenommen, wenn am Ende der Rekonfiguration nach Regel 15 oder Regel 16 eine Ausgliederung erfolgt.

(Hinweis: Eine redundante Station, die replika-deterministisch arbeiten, jedoch keine Ausgaben produzieren soll (hot stand by) muß im Normalbetrieb im Sendmodus SendOnNoBus arbeiten, da im Passivbetrieb kein VETO möglich ist).

Regel 18

Gelangt eine Station in den Passivbetrieb, setzt sie sich selbst im lokalen Zustandsvektor excluded. Im Passivbetrieb werden keine Nachrichten und keine VETO-Signale gesendet. Nachrichten anderer Stationen werden der Anwendung nach Regel 9 übergeben. Nachrichten, die nur von der eigenen Station inkorrekt empfangen wurden und nicht invalidiert werden, gehen verloren; die Anwendung bekommt eine Fehlermeldung.

Regel 19

Eine Station muß zunächst, wenn sie direkt in den Passivbetrieb gestartet wird, den aktuellen Zyklus und ihre eigene Zeitscheibe in Erfahrung bringen. Die Station muß außerdem den aktuellen Systemzustand bestimmen. Wird bei Ankunft einer Protokollnachricht eine unterschiedliche Prüfsumme erkannt (Abweichung der Zeitscheibenvergaben im System mit den eigenen Zeitscheibenvergaben), schaltet sich die Station ab.

Regel 20

Nummer des aktuellen Zyklus (Mode) bestimmen: Dazu wertet die Station nacheinander die Cycle-Bits aller Normal-Frames mit Applikationsnachricht aus, die nicht invalidiert werden. Bekommt sie eine Protokollnachricht gilt unmittelbar Regel 23. Bekommt sie aber ein gestörtes Frame, das nicht invalidiert wird, oder ein Recovery-Frame, muß sie die Auswertung neu beginnen. Eine Sequenz beginnt mit einer ersten 0 (Anfangskennung) im Cycle-Bit und ist vollständig, wenn eine zweite 0 (Endekennung) erkannt wird. Die Nummer des Zyklus ergibt sich aus der Summe unmittelbar aufeinander folgender Normal-Frames mit einer 1 im Cycle-Bit.

Regel 21

Zeitscheiben bestimmen: Setzt man die eigene statische Zeitscheibenvergabe zunächst als konsistent mit dem System voraus, kann die beobachtende Station einzelne Zeitscheiben im aktuellen Zyklus inspizieren und die Slice-Bits der darin gesendeten Normal-Frames mit Applikationsnachricht auswerten. Eine Sequenz ist gültig, wenn die beobachtete Zeitscheibe nicht gestört wird, also Normal-Frames in Folge gesendet werden. Die erste abgeschlossene 0 (Anfangskennung) bis 0 (Endekennung)-Sequenz läßt die Nummer der Zeitscheibe erkennen, die sich aus der Summe unmittelbar aufeinander folgender Normal-Frames der Zeitscheibe mit einer 1 im Slice-Bit ergibt. Damit ist/sind auch die eigene/n Zeitscheibe/n im Zyklus bestimmt. Bei nicht-redundanten Stationen dürfen in dieser/n Zeitscheibe/n keine anderen Stationen senden. Mit Hilfe der Zeitscheibennummer kann wegen der global konsistenten Zeitscheibenvergabe auf die Stationsadresse geschlossen werden und Regel 22 durchgeführt werden. Bekommt die Station in dieser Zeit eine Protokollnachricht gilt ebenfalls unmittelbar Regel 23.

Regel 22

Systemzustand bestimmen: Die Station setzt alle Stationen im Systemzustandsvektor excluded. Sie beobachtet dann mindestens einen ungestörten TDMA-Zyklus lang das Nachrichtengeschehen (nur N-Frames werden gesendet) und setzt alle Stationen included, deren Zeitscheibe nicht durch VETO invalidiert wird. Regel 22 kann parallel zu Regel 21 durchgeführt werden und ebenfalls abgebrochen werden, wenn eine Protokollnachricht empfangen wird.

Regel 23

Wird ein Frame mit Protokoll-Nachricht empfangen, kann der aktuelle Zyklus, die aktuelle Zeitscheibe und der Zustandsvektor übernommen werden. Die Regeln 20, 21 und 22 können ausgesetzt werden.

Regel 24

Die Anwendung kann einen Wechsel vom Passivbetrieb über die Eingliederung in den Normalbetrieb veranlassen, wenn die Station im aktuellen Zyklus eine eigene Zeitscheibe besitzt. Ging dieser Aufforderung eine protokoll-gesteuerte Ausgliederung nach Regel 15 voran, führt sie den Zustandswechsel nur dann aus, wenn sie eine bestimmbare Zeitdauer "t" lang keine gestörten Frames empfangen hat und die Anzahl der eigenen Ausgliederungen pro vorangegangener Zeiteinheit "T" einen gegebenen Schwellwert nicht überschritten hat ("t"

und "T" muß noch festgelegt werden).

Regel 25

Eine Station im Normalbetrieb kann von der Anwendung jederzeit in den Passivbetrieb geschaltet werden. Der Passivbetrieb wird sofort wirksam.

4.5 Eingliederung

Regel 26

Stationen im Zustand Eingliederung senden grundsätzlich kein VETO-Signal.

Regel 27

a) Wenn eine Station nicht direkt aus dem Passivbetrieb kommt, muß sie zunächst nach Regel 20, 21 und 22 den aktuellen Zyklus, ihre Zeitscheibe und den aktuellen Systemzustandsvekor bestimmen. Nachrichten werden nach Regel 9 an die Anwendung weitergeleitet, sobald die aktuelle Zeitscheibe und der Zyklus bekannt sind. Besitzt die Station im Zyklus keine eigene Zeitscheibe, so geht sie unmittelbar in den Passivbetrieb.
b1) Ist eine Station bereits nach Durchführung von Regel 27a included gesetzt (redundanter Partner aktiv), geht sie sofort in den Normalbetrieb, siehe auch Regel 38. Sobald ihr der redundante Partner über das B-Bit des Protokollbyte signalisiert (oder signalisiert hat), daß der zum Senden befohlene Bus frei ist, geht sie in den befohlenen Sendemodus. Solange der Bus besetzt ist sendet sie nicht: Sendemodus SendOnNoBus.
b2) Ist die Station nicht included sendet sie, wenn das laufende Protokoll im Normalbetrieb ist, in ihrer ersten nachfolgenden Zeitscheibe ein N-Frame mit Protokollnachricht vom Typ INTEGRATE. Wird zwischenzeitlich ein Zykluswechsel wirksam, wird der neue Modus übernommen und überprüft. Besitzt die Station im neuen Zyklus keine eigene Zeitscheibe, so geht sie unmittelbar (wieder) in den Passivbetrieb.
c1) Wird das Frame nicht invalidiert, ist die Station integriert und befindet sich unmittelbar im Normalbetrieb. Sie wird in allen Stationen included gesetzt, und die Anwendung bekommt eine Mitteilung (SYSCHANGE) (vgl. Bild 16).
c2) Im anderen Fall versucht die Station frühestens nach jeweils "m" TDMA-Zyklen, wenn keine Störungen aufgetreten sind, "n" weitere Eingliederungen nach Regel 27 ("m" und "n" muß noch festgelegt werden) und führt zuvor die Regel 20, 21 und 22 nochmals durch. Nach "n" Versuchen geht sie in den Passivbetrieb.

Regel 28

Wird von einer included gesetzten Station ein Normal-Frame mit Protokollnachricht vom Typ INTEGRATE empfangen, wird der enthaltene Zyklus, die Zeitscheibe, der Systemzustandsvektor und die Prüfsumme der Zeitscheibenvergaben mit den eigenen Werten verglichen. Im Fall einer Differenz, wird die Nachricht durch VETO-Signal invalidiert.

Regel 29

Empfängt eine Station in der Eingliederung einen TDMA-Zyklus lang kein Frame, geht sie in die Initialisierung.

4.6 Zykluswechsel

Regel 30

Gelangt eine Station im Normalbetrieb in ihre Zeitscheibe sendet sie eine Protokollnachricht vom Typ CHMODE, wenn ihr ein entsprechender Wunsch von der Applikation vorliegt. Die Protokollnachricht enthält die Nummer des angeforderten Zyklus, die Nummer der anzuspringenden Zeitscheibe im neuen Zyklus und den aktuellen Systemzustandsvektor, worin jedoch alle Stationen, die im angeforderten Zyklus keine eigene Zeitscheibe besitzen, excluded gesetzt sind.

Regel 31

Empfängt eine Station im Normalbetrieb eine Protokollnachricht vom Typ CHMODE überprüft sie, ob der angeforderte Zyklus zuvor von der eigenen Applikation freigegeben wurde. Ist das nicht der Fall, sendet sie VETO, wenn sie im angeforderten Zyklus eine Zeitscheibe besitzt. Eine mit VETO bedachte CHMODE-Nachricht wird generell verworfen. Danach wird nach Regel 14 ein Rekonfigurationszyklus durchgeführt, so daß ein erneuter Zykluswechsel zunächst verhindert wird.
Wird die CHMODE-Nachricht nicht mit VETO quittiert, übernehmen alle Stationen den gesendeten Systemzustandsvektor; Stationen die dabei excluded gesetzt werden gehen in den Passivbetrieb. Unmittelbar nach Ablauf der aktuellen Zeitscheibe beginnt die angeforderte Zeitscheibe im neuen Zyklus. Stationen, die im Vorzyklus nicht included gesetzt waren, jedoch nun beteiligt und nicht permanent ausgegliedert sind, werden in

den Zustand Eingliederung versetzt.

Im folgenden Beispiel werden Zykluswechsel durchgeführt, die die Aus- und Eingliederung einer Station (6) bewirken. Dazu wird abermals die Idee eines Leitsystems im zukünftigen Kfz bemüht, das aus einer redundanten Fahrerstation 0 und den Radstationen 1 bis 4 besteht. Die Station 5 sei beispielsweise das Getriebemanagement und die Station 6 das Motormanagement mit der Funktion Anfahrschlupfregelung. Nachrichten dieser Regelungsfunktion sind bei Schnellfahrt ohne Bedeutung; die Station wird ausgegliedert, um den Bremsregelzyklus zu verkürzen (Mode 1). Sie wird bei langsamer Fahrt wieder eingegliedert (Mode 2).

Zeitscheibe	0	1	2	3	4	5	6	7	8
Mode 1	0	0	5	1	2	3	4	0	1 ...
Mode 2	0	0	5	1	2	3	4	6	0 1 ...

Die Zeitscheibe 2 (Station 5) läßt der Radstation 1 nach dem Kommando der Fahrerstation 0 Rechenzeit zur Reaktion und Antwort. Die Station 0 besitzt (außer ihren redundanten Zeitscheiben am Beginn) jeweils am Ende der Zyklen eine weitere Zeitscheibe, in der sie keine Anwendernachrichten sendet. Daher werden in dieser Zeitscheibe vom Protokoll Nachrichten vom Typ NULL gesendet, die eine schnelle (Wieder-)Eingliederung von Stationen gestatten. Die Fahrerstation 0 nutzt diese Zeit zum Auswerten der Antwort der Radstationen, bevor sie im neuen Zyklus Kommandos sendet. Diese Zeitscheibe wird von ihr auch benutzt um Zykluswechsel durchzuführen.

Bild 17 zeigt den Ablauf des Protokolls nach dem Mode-Change-Request:
Ein Zykluswechsel zur Eingliederung der Station 6 erfolgt von der Zeitscheibe 7 des Mode 1 in die Zeitscheibe 7 des Mode 2, um der Station 6 eine sofortige Anmeldung zur Eingliederung zu gestatten, siehe Bild 17. Zum Rücksprung aus dem Mode 2 wird ein Zykluswechsel aus der Zeitscheibe 8 in den Mode 1 Zeitscheibe 0 durchgeführt. Die Ausgliederung der Station 6 erfolgt dabei automatisch.

4.7 Maßnahmen zur Erhaltung der Konsistenz

Regel 32

VETO-Signale (und ihre Hardware) sind so zu implementieren, daß sie mit sehr hoher Wahrscheinlichkeit, auch unter starken Störeinflüssen, erkannt werden. Dabei ist es zulässig, daß die Erkennungs-Hardware einzelne Störungen als VETO interpretiert und meldet, was dann nach Regel 4 global bekannt gemacht wird. Es ist nicht zulässig, daß ein VETO-Signal durch eine mögliche Störung nicht erkannt wird.

Regel 33

VETO wird von der Empfangs-Hardware erkannt. Damit ist der Fall, daß eine Station ein Frame korrekt empfängt, ein nachfolgendes VETO-Signal jedoch nicht erkennt, extrem unwahrscheinlich, kann jedoch durch einen transienten Fehler verursacht werden. Ein permanenter Fehler würde (zumindest nachfolgend) beide Funktionen — Empfang von Frames und Veto-Erkennung — stören.

Die folgenden Maßnahmen sind geeignet das Restrisiko aus Regel 33 abzudecken. Sie sind sehr einfach zu implementieren und bewirken, daß die Konsistenz im System nach einem solchen Fehler innerhalb eines Zyklus wiederhergestellt ist:

Regel 34

Regel 11 wird erweitert: Im Quittungsfenster einer excluded gesetzten Station wird auch dann VETO gesendet, wenn die Station ein Frame gesendet hat, das nicht vom Typ INTEGRATE-Protokollnachricht ist. (Bei Empfang einer INTEGRATE-Protokollnachricht siehe Regel 28).

Regel 35

Empfängt eine Station, nach einer korrekten, nicht-invalidierten Übertragung eines Normal-Frame, ein Recovery-Frame, verbleibt sie im Normalbetrieb.

Regel 36

Empfängt eine Station, die sich im Rekonfigurationszyklus befindet, ein Normal-Frame von einer Station, die nicht der eingangs gestörte Sender ist, wertet sie das Frame wie ein R0-Frame. Handelt es sich beim Normal-Frame um eine Protokollnachricht vom Typ CHMODE, wird die Zeitscheibe durch VETO invalidiert.

Die Bilder 18 bis 21 geben den Refigurationszyklus einzelner Stationen und die Anwendung der Regeln 34, 35, 36 sowie (im Einzelfall) der Regeln 11, 14, 16 wieder.

4.8 Unterstützung redundanter Stationen

Grundsätzlicher Aufbau redundanter Stationen

Im allgemeinen Fall besitzen Stationen neben der Kommunikationsschnittstelle eine auch Schnittstelle zum Technischen Prozeß. Werden Sensordaten eingelesen, müssen Stationen, die in aktiver Redundanz arbeiten, diese Eingaben miteinander abgleichen und, wenn Alternativen vorhanden sind, ihre nächsten Aktionen abstimmen (Replika-Determinismus). Außerdem sollen sie u. U. auch ihre Ergebnisse vergleichen oder votieren, bevor sie weitergegeben werden. In jedem Fall ist Kommunikation untereinander notwendig. Redundante Stationen, die jeweils eine eigene Zeitscheibe besitzen, können natürlich ohne Probleme über den Systembus miteinander kommunizieren. Bei dieser Kommunikationsart werden jedoch viele Zeitscheiben benötigt, wodurch der Sendezugriff im Gesamtsystem verzögert wird. Will man Abgleich und Synchronisation aus Geschwindigkeits- und Lastgründen nicht über den Systembus abwickeln, benötigen redundante Stationen zusätzliche lokale Kommunikationsquerverbindungen (vgl. **Bild 22**).

Lokale "Punkt zu Punkt"-Querverbindungen sind vernünftig,

— weil redundante Stationen meist am selben Ort und vielleicht im selben Gehäuse plaziert sind, die Querverbindungen daher kurz und nirgendwo im Wege sind,
— weil sie einfach implementiert werden können und daher kostengünstig sind,
— weil der Systembus stark entlastet wird,
— weil praktisch keine Verzögerung beim Abgleich mit redundanten Partnern entsteht, so daß auch schnelle lokale Regelungen in den Stationen durchgeführt werden können,
— weil die Ausfalloffenbarungszeit redundanter Partner verkürzt wird und
— weil der Sicherheitsnachweis erheblich vereinfacht wird.

Kommunikation redundanter Stationen mit gemeinsamer/n Zeitscheibe/n

Ein redundanter Stationsverbund kann eine oder zwei aufeinander folgende gemeinsame Zeitscheibe/n erhalten, in der/denen eine oder zwei ausgewählte Stationen die externen Nachrichten versenden. Die übrigen Stationen des redundanten Verbundes senden nicht,
sind jedoch VETO-berechtigt, erhalten dadurch alle Nachrichten, auch die ihrer Partnerstationen, und können dem aktuellen Geschehen folgen.

Die Protokollmaschine ist, mit ihren verschiedenen Sendemodi (siehe Regel 38), gut ausgerüstet, die Kommunikation für redundante Stationen in einer oder zwei Zeitscheibe/n durchzuführen. Die Stationen können dabei in den verschiedensten Redundanzstrategien, wie Duplex, Duplex mit Backup, Triple-Modular-Redundancy und Doppel-Duplex, am Systembus gleichzeitig arbeiten. Die Strategien werden in einer Software-Schicht (Redundanzmanagement) abgebildet, die die Sendemodi der Protokollmaschine steuert.

Wird ein nicht-redundanter Systembus verwendet, kann nur eine der redundanten Stationen in einer zugeordneten Zeitscheibe senden. Bei einem redundanten Bus, der aus zwei Leitungen besteht, ist auch die Betriebsart "zwei Stationen senden auf je einer Leitung" möglich. Alle weiteren redundanten Stationen senden in dieser Zeitscheibe nicht, legen jedoch ggf. VETO ein. Es werden folgende verfeinerte Betriebsarten für einen redundanten Bus vorgeschlagen, siehe dazu **Bild 26**:

Betriebsart 1

Eine primäre Station sendet auf dem redundanten Bus, solange keine Störung auftritt. Eine redundante Station tritt nach Ausfall der Primärstation in Aktion.

Betriebsart 2

Zwei redundante Stationen senden gleichzeitig auf je einer Leitung des redundanten Busses. Es kann ein Vergleich der Nachrichten beim Empfänger durchgeführt werden.

Betriebsart 3

Zwei redundante Stationen senden gleichzeitig auf je einer Leitung des redundanten Busses und in der nachfolgenden Zeitscheibe umgekehrt (Vorschlag aus TTP). Eine einfache Störung kommt nicht durch und es kann ein Vergleich der Nachrichten beim Empfänger durchgeführt werden.

Betriebsart 4 und 5

TMR und DoppelDuplex/Quadruplex-Betrieb

In der Betriebsart 1 gibt es den Nachteil, das die Sendeeinrichtung des redundanten Knotens nicht laufend überprüft werden kann, ein Ausfall unbemerkt bleibt und eine Übernahme ggf. nicht möglich ist. Für redundante Stationen, an die die Anforderung gestellt wird fail-operational zu arbeiten, ist diese Betriebsart nicht zulässig.

In der Betriebsart 2 bis 5 gibt es einen Nachteil bei ereignisgesteuerter Anwender-Software: Geringe Laufzeitunterschiede in den redundanten Stationen können dazu führen, daß die Protokollmaschine der einen Station die Nachricht gerade noch vor dem Sendezeitpunkt bekommt und in Form einer Anwendernachricht auf ihre Busleitung bringt, während die Protokollmaschine der anderen Station, der zum Sendezeitpunkt noch keine Anwendernachricht vorliegt, eine Protokollnachricht des Typs NULL auf ihrer Leitung sendet. Da ein solches Ereignis auch von den Sendern selbst erfaßbar ist, indem die Sendungen der eigenen Zeitscheibe von der

Applikation ausgewertet werden, kann die Anwendung konsistent reagieren.

Regel 37

Regel 14 (Rekonfigurationszyklus) wird ausgesetzt und der Normalbetrieb fortgeführt, wenn die nachfolgende Zeitscheibe der gleichen Station gehört oder wenn die vorangegangene Zeitscheibe der gleichen Station gehört und ungestört blieb (s. Bilder 23 bis 25).

Regel 38

Wird einer included gesetzten Station ein neuer Sendemodus befohlen, wird er unmittelbar in der nächsten eigenen Zeitscheibe ausgeführt. Folgende Sendemodi sind möglich:
SEND_NONE: nicht senden (jedoch VETO)
SEND_ANY: in jeder Zeitscheibe auf beiden Bussen senden (Voreinstellung), beim Senden wird das B-Bit im Protokollbyte gesetzt
SEND_BUS1/2: auf Bus 1/2 senden
SEND_EVEN/ODD: in gerader/ungerader Zeitscheibe auf beiden Bussen senden
SEND_CROSSWISE1: in gerader Zeitscheibe auf Bus 1, in ungerader auf Bus 2 senden
SEND_CROSSWISE2: in gerader Zeitscheibe auf Bus 2, in ungerader auf Bus 1 senden
SEND_BUS1EVEN: in gerader Zeitscheibe auf Bus 1 senden
SEND_BUS1ODD: in ungerader Zeitscheibe auf Bus 1 senden
SEND_BUS2EVEN: in gerader Zeitscheibe auf Bus 2 senden
SEND_BUS2ODD: in ungerader Zeitscheibe auf Bus 2 senden
(Anmerkung: Wird von der Anwendung — durch gleiche Einstellung der redundanten Protokollmaschinen — eine totale Kollision (oder Aussetzer) produziert, werden alle redundanten Stationen ausgegliedert).

Regel 39

Eine redundante Station gliedert sich wieder ein, auch wenn ihre Adresse bereits included gesetzt ist. Sie sendet eine Nachricht vom Typ INTEGRATE in ihrer zugewiesenen Zeitscheibe und auf ihrem(n) Bus(sen). Die redundanten aktiven Partnerstationen senden als Bestätigung der Eingliederung in der nächsten nachfolgenden Zeitscheibe ein Frame mit gesetztem R-Bit.

In Bild 26 sind redundante Sendemodi der Betriebsarten 2, 3, 4 und 5 dargestellt.

4.9 Untersuchung von Mehrfachfehlern

Hierzu geben die Bilder 27 bis 29 Beispiele an.

4.10 Aufbau der Kommunikations-Hardware

Ohne dem genauen Design der Kommunikations-Hardware mit der Protokollmaschine (Protocol Engine) vorgreifen zu wollen, sei nachfolgend in Verbindung mit Bild 30 eine prinzipielle Idee zum möglichen Aufbau der Kommunikationshardware dargestellt.

Jede Station besitzt zur Vermeidung von Common-Mode-Fehlern im Zeitbereich zwei unabhängige Uhrenbausteine, die aus einer Timer-Sektion und einem Window-Generator bestehen. Eine dieser Uhren generiert die Interrupts AT_NEXTSLICE (Beginn eines neuen Zeitfensters) und AT_VETO (Beginn des Quittungsfensters) für die Protokollmaschine. Die Window-Generatoren beider Uhren (oder auch nur einer) produzieren Transmit Windows und wirken so als "Time-Guardian" auf die Sende-Hardware (Transmitter) der Station. Die Uhrenbausteine werden von der Protokollmaschine angestoßen, arbeiten jedoch weitgehend autonom (unter Zuhilfenahme von Information im Dual-Port-RAM: DPR). Weicht ein Uhrenbaustein zu stark vom anderen ab, oder die Protokollmaschine hält die vorgegebenen Zeiten nicht ein, werden die eigenen gesendeten Nachrichten zerstört und die Station wird ausgegliedert bzw. gliedert sich selbst aus.

Das Watchdog-Signal ist optional und wird generiert, wenn die Protokollmaschine die Uhren nicht regelmäßig anstößt. Eine Uhr produziert keine Transmit-Windows mehr, sobald sie das Watchdog-Signal sendet. Mit dem Watchdog-Signal wird die Protokollmaschine zurückgesetzt. Auf dieses Signal muß anwenderseitig reagiert werden. Des weiteren sollten die Transmit-Windows der Uhren laufend (u. U. von der Protokollmaschine) auf "stuck at 1" überprüft werden (nicht im Bild enthalten), da ein unerkannter Fehler in den Sicherungseinrichtungen unbedingt aufgedeckt werden muß.

4.11 Vorläufige Synchronisation des Protokolls

Nachfolgend wird ein einfaches Prinzip zur Synchronisation der Protokollmaschinen und zur Erzeugung der Interrupts AT_NEXTSLICE und AT_VETO für den ersten Kommunikationsprototypen vorgestellt, das nicht den Anspruch erhebt einen sicheren Betrieb zu gewährleisten, jedoch eine erste praktische Erprobung (bei F3S/R) ermöglicht.

Regel 40 (vorläufig)

Die Interrupt-Uhr besteht aus 2 Registerpaaren (Timern), ein Paar wird gebildet aus einem aktuellen Countdown-Zähler und einem Zyklusregister. Die Zähler beider Paare werden von einem gemeinsamen Takt getrieben. Der Zähler läuft, sobald er geladen wird, und löst, wenn er den Wert 0 erreicht hat, einen Interrupt aus. Der Inhalt des Zyklusregisters wird danach automatisch in den Zähler geladen.

In die Zyklusregister der beiden Timer kommt das Zeitäquivalent für eine Zeitscheibe $\{T_{Slice}\}$, Unmittelbar nach Empfang des ersten korrekten Frames wird der Zähler des Timers AT_NEXTSLICE mit dem Zeitäquivalent für das Quittungsfenster plus der Uhrenabweichung im System $\{T_{VETO} + \Delta T_{Tick}\}$ geladen und der Timer AT_VETO mit dem Zeitäquivalent für eine Zeitscheibe plus Uhrenabweichung $\{T_{Slice} + \Delta T_{Tick}\}$ geladen. Jedesmal, wenn danach ein Frame einer fremden included gesetzten Station korrekt empfangen wird und der Timer AT_VETO eine Differenz $D < \Delta T_{Tick} - \varepsilon$ oder $D > \Delta T_{Tick} + \varepsilon$ aufweist, werden die Timer nach diesem Mechanismus gestellt. Wird jedoch zu zwei verschiedenen Sendern eine Differenz $D < \Delta T_{Tick} - \sigma$ oder $D > \Delta T_{Tick} + \sigma$ festgestellt, wobei gilt $\Delta T_{Tick} > \sigma > \varepsilon$, wird die Protokollmaschine abgeschaltet, da die Abweichung der internen Taktfrequenz zu groß ist.

Eine Station beginnt in ihrem Zeitfenster mit der eigenen Sendung, wenn der Timer AT_NEXTSLICE den Wert $\{T_{Slice} - T_{Tick}\}$ erreicht hat (t_{Send}).

In Bild 31 ist ein Zeitdiagramm der Synchronisation dargestellt.

5. Literatur

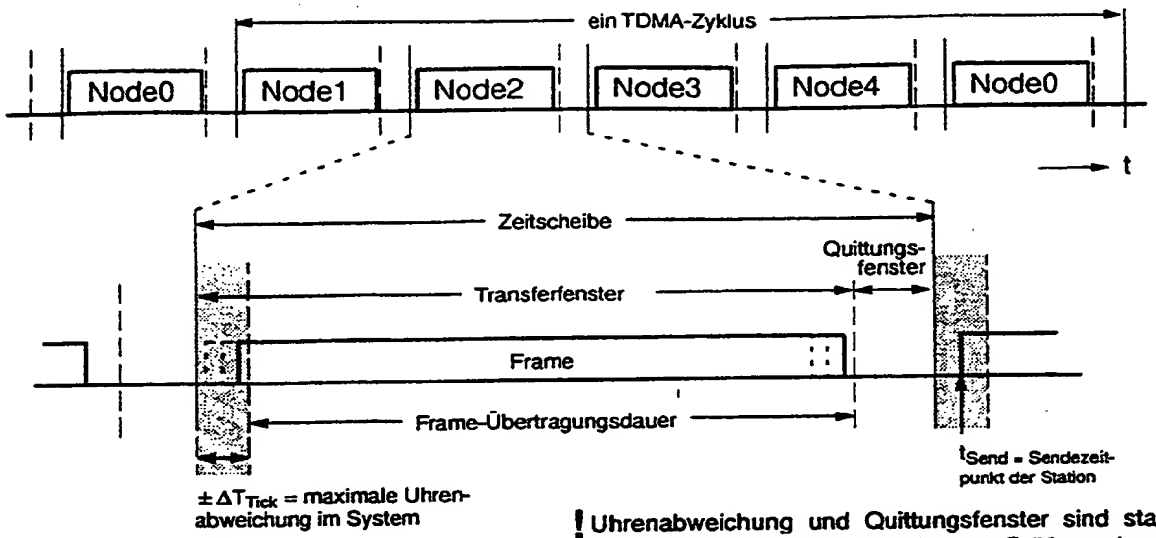
[1] SAE Handbook Volume 2, Parts and Components:
Class C Application Requirement/Survey of known Protocols, S 23. 366 ff, 1994
[2] ISO 11 898: Road vehicles — Interchange of digital information — Controller area network (CAN) for high-speed communication, 1993
[3] Telefunken Electronics:
Automotive Bit-serial Universal-interface System (ABUS), 8/1988
[4] IEC TC9 WG 22:
Train Communication Network (1. General Architecture, 2. Real-Time Protocols, 3. Multifunction Vehicle Bus, 4. Wire Train Bus), Working Document 3/1994
[5] H. Kopetz, W. Ochsenreiter:
Clock Synchronization in Distributed Real-Time Systems, IEEE Transactions on Computers, Vol. C-36, No. 8, 8/1987
[6] H. Kopetz, W. Ochsenreiter:
Clock Synchronization UNIT (CSU) Datasheet, Research Report 22/89, Technische Universität Wien, November 1989
[7] K. Hoyme, K. Driscoll:
SAFEbus™ Honeywell Systems and Research Center, (Draft in ARINC 659, Boing 777), IEEE AES Systems Magazine, 3/1993
[8] H. Kopetz, G. Grünsteidl:
TTP- A Time Triggered Protocol for Automotive Applications, Technische Universität Wien, 10/1992 bzw. The 23rd International Symposium on Fault-Tolerant Computing, Toulouse 6/1993
[9] ISO/IEC 8802-4, ANSI/IEEE Std 802.4:
Token-Passing Bus Access Method and Physical Layer Specifications, 1990
[10] IEEE Std 802.5:
Token Ring Access Method and Physical Layer Specifications, 1989
[11] ISO/IEC 8802-3, ANSI/IEEE Std 802.3:
Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, 1990

Patentansprüche

Protokoll zur Übertragung von Nachrichten zwischen sendenden und empfangenden Stationen in Zeitscheiben für sicherheitskritische Anwendungen auf der Basis einer synchronen Arbitration, **dadurch gekennzeichnet,**
daß die Zeitscheiben zyklisch jeweils einer Empfangsstation durchgängig deterministisch zugeordnet werden,
daß die Zeitscheiben jeweils in ein zeitliches Transferfenster zur Übertragung der Nachricht bzw. einer Teilnachricht und in ein an das Transferfenster anschließendes zeitliches Quittungsfenster unterteilt werden und daß im Quittungsfenster ausschließlich bei einer fehlerhaft oder gar nicht empfangenen Nachricht von der Empfangsstation ein Einspruchssignal (VETO-Signal) als Anzeige einer Störung abgegeben wird.

Hierzu 11 Seite(n) Zeichnungen

Nummer: DE 196 20 137 A1
Int. Cl.[6]: H 04 L 29/06
Offenlegungstag: 13. November 1997



! Uhrenabweichung und Quittungsfenster sind stark vergrößert dargestellt (geschätzte Größenordnung des Quittungsfensters: < Übertragungszeit für 1 Byte).

Bild 1 Ungestörter Betrieb

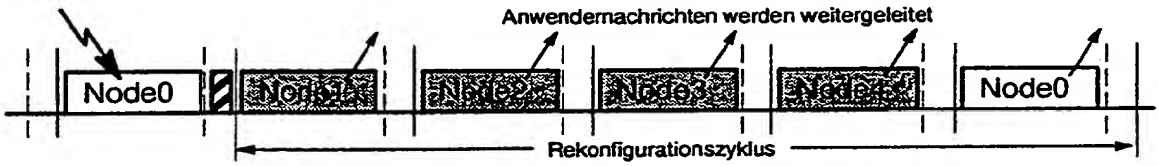


Bild 2 Einzelstörung (Sendefehler oder Störung)

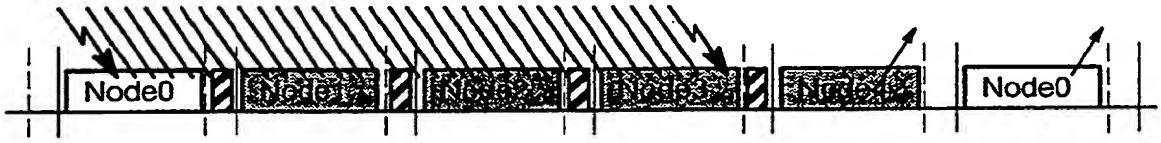


Bild 3 Anhaltende Störung (Burst-Störung)

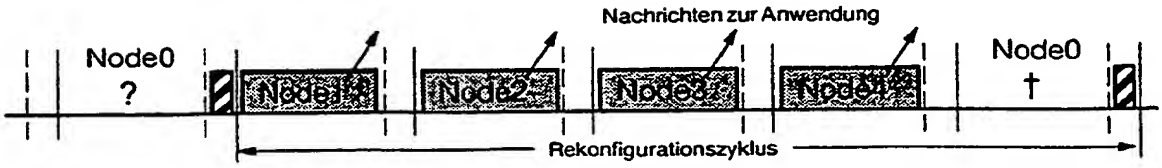


Bild 4 Ausfall einer Station (oder permanenter Sendefehler)

Nummer: DE 196 20 137 A1
Int. Cl.[6]: H 04 L 29/06
Offenlegungstag: 13. November 1997

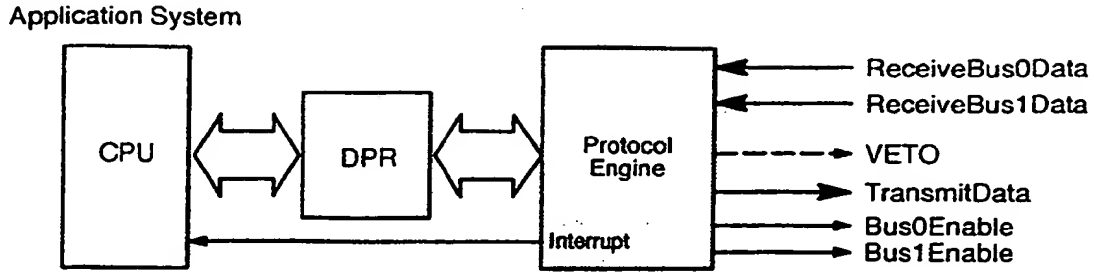


Bild 5 Anschlüsse der Protokollmaschine

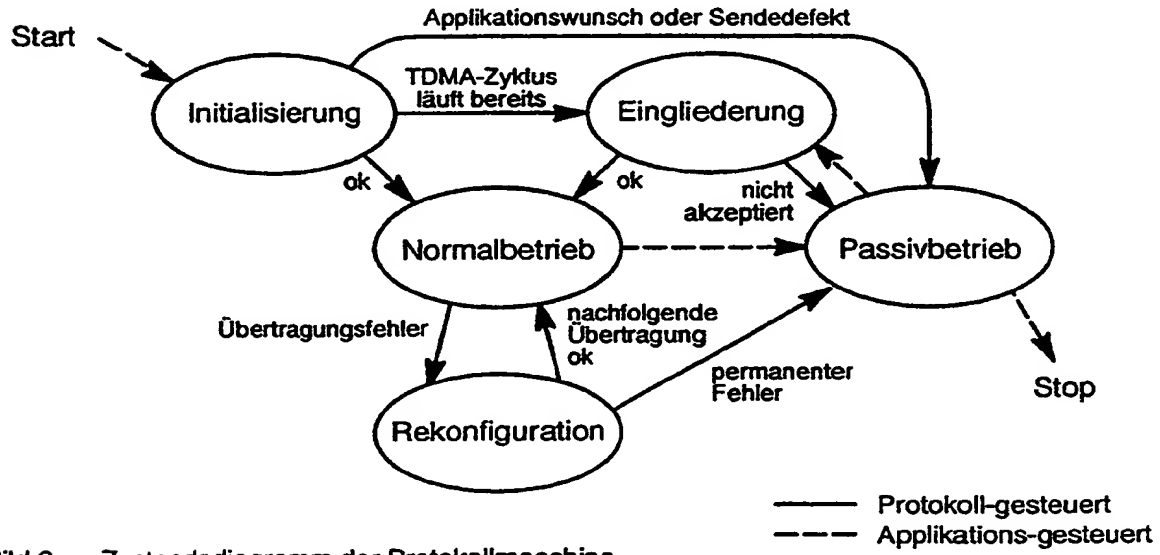


Bild 6 Zustandsdiagramm der Protokollmaschine

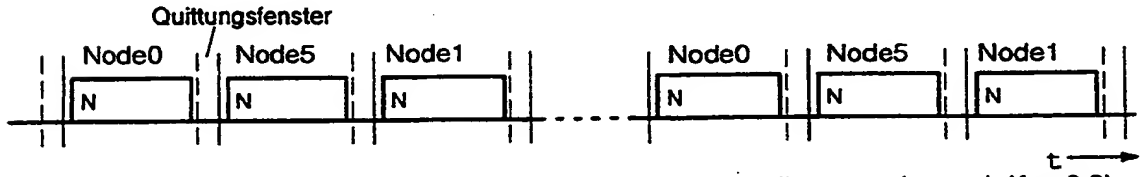


Bild 7 Ablauf des Protokolls im ungestörten Betrieb (Zeitscheibenvergabe nach Kap.2.2)

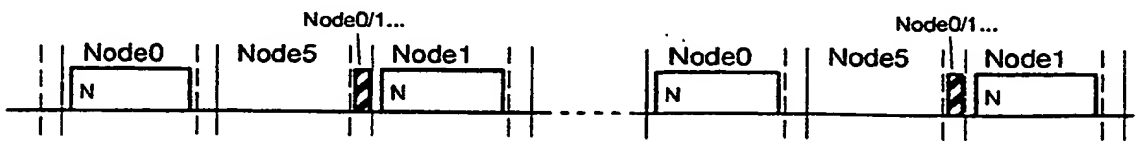


Bild 8 Ablauf des Protokolls bei inaktiver Station (Node5)

Nummer: DE 196 20 137 A1
Int. Cl.[6]: H 04 L 29/06
Offenlegungstag: 13. November 1997

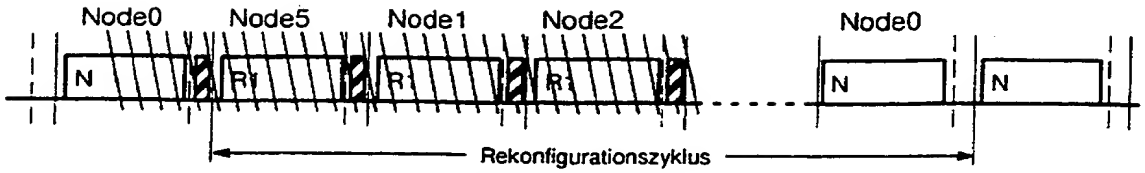


Bild 9 Anhaltende Störung im Rekonfigurationszyklus

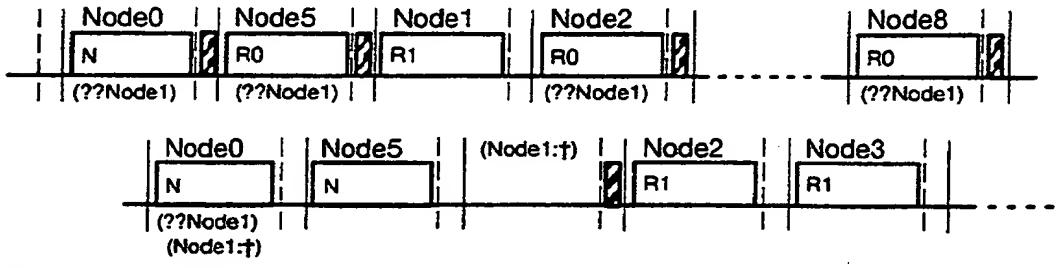


Bild 10 Ablauf des Protokolls bei permanent defektem Empfangskanal: Node1

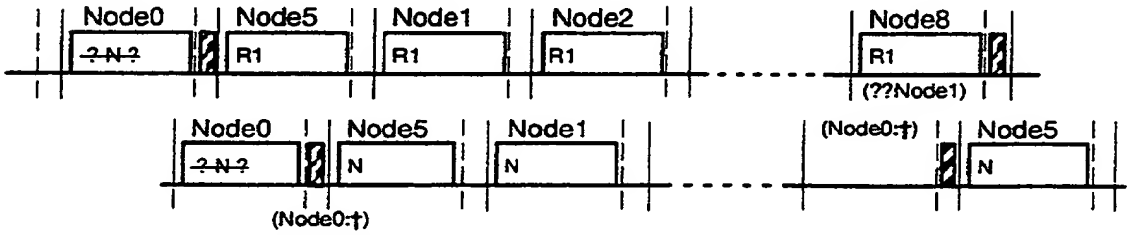


Bild 11 Ablauf des Protokolls bei permanent defektem Sendekanal: Node0,
gleicher Ablauf bei Totalausfall des Senders: Node0

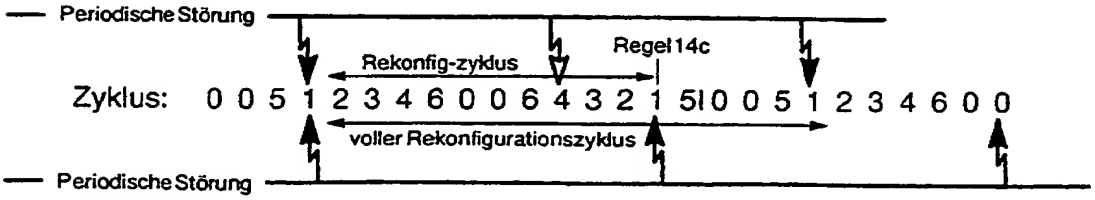


Bild 12 Asymetrischer Zyklus vermeidet Ausgliederungen durch periodische Störungen

Nummer: DE 196 20 137 A1
Int. Cl.[6]: H 04 L 29/06
Offenlegungstag: 13. November 1997

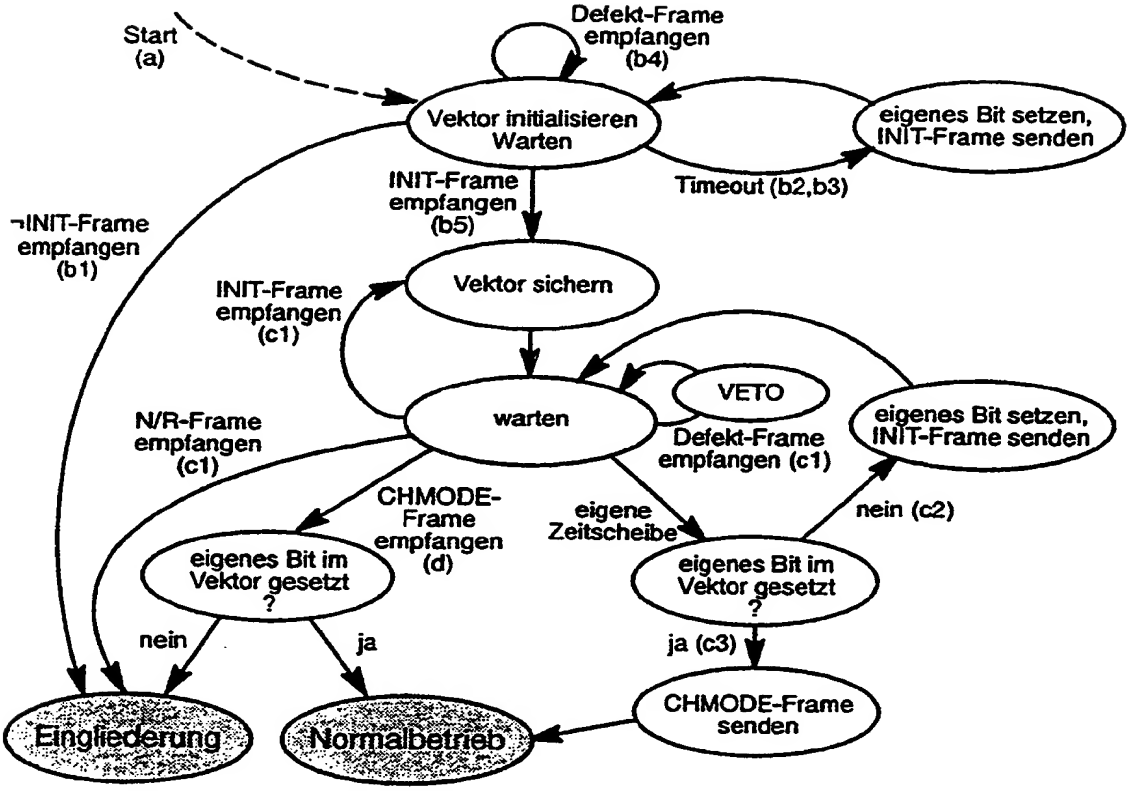


Bild 13 Zustandsdiagramm der Initialisierung

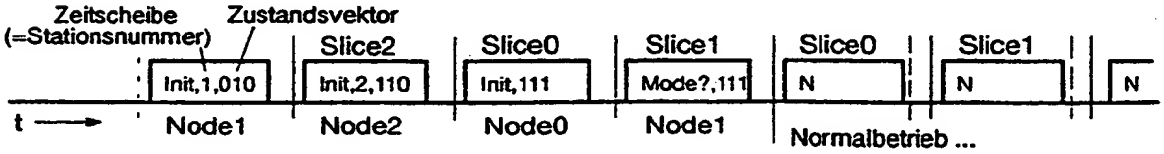


Bild 14 Normaler Start des Protokolls (3 Stationen im Zyklus, Node1 sendet zuerst)

Nummer: DE 196 20 137 A1
Int. Cl.[6]: H 04 L 29/06
Offenlegungstag: 13. November 1997

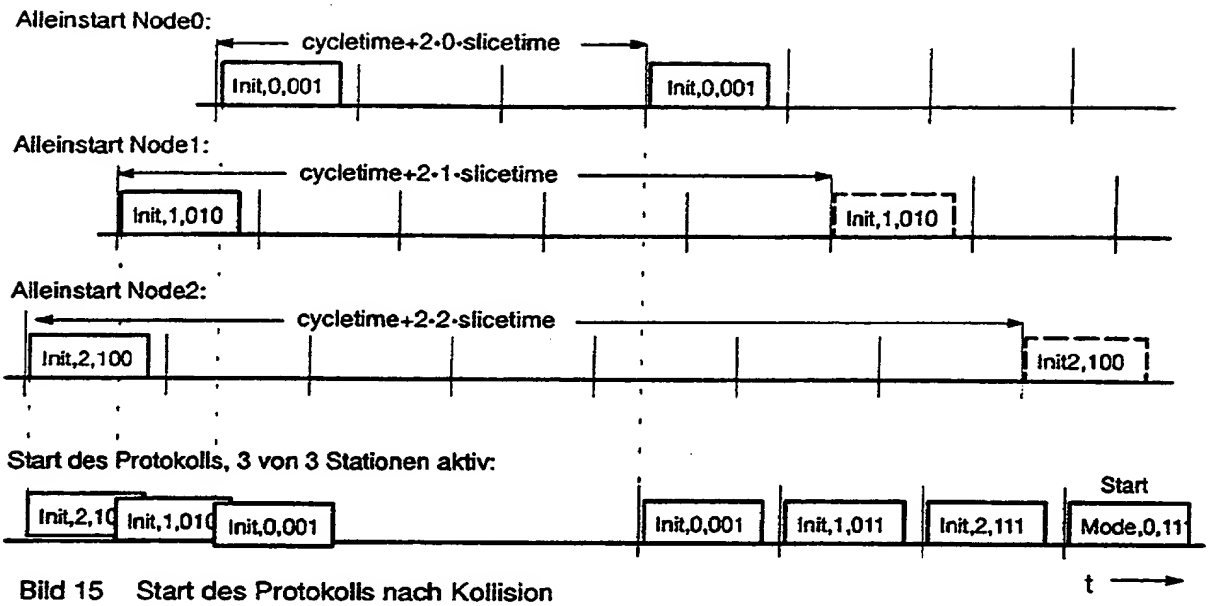


Bild 15 Start des Protokolls nach Kollision

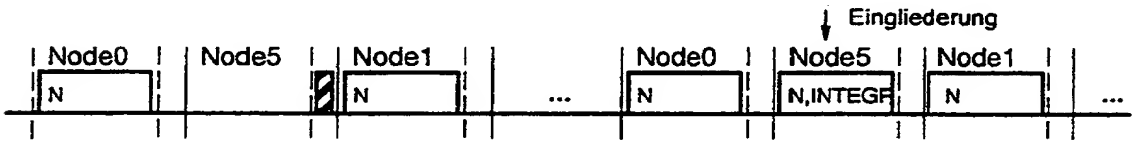


Bild 16 Ablauf des Protokolls bei (Wieder-)Eingliederung einer Station

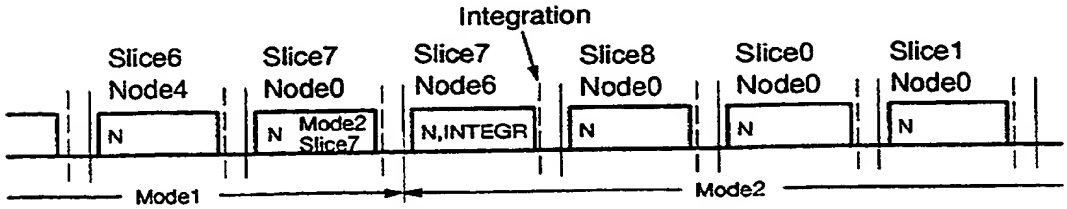


Bild 17 Ablauf des Protokoll nach Mode-Change-Request

Nummer: DE 196 20 137 A1
Int. Cl.[6]: H 04 L 29/06
Offenlegungstag: 13. November 1997

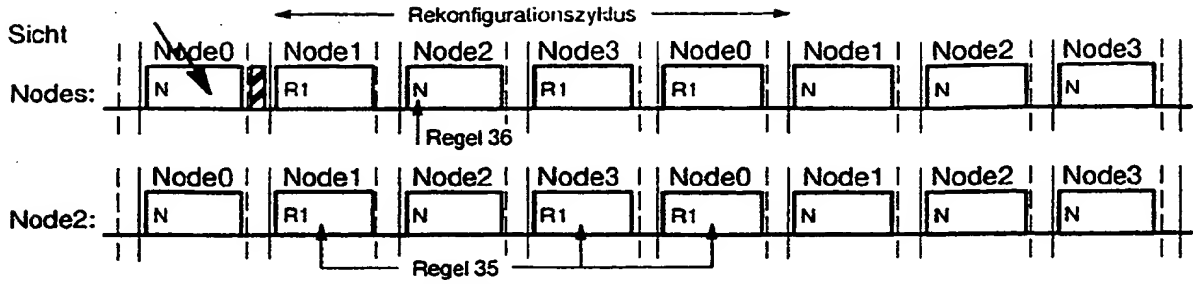


Bild 18 Station (2) empfängt N-Frame jedoch kein VETO

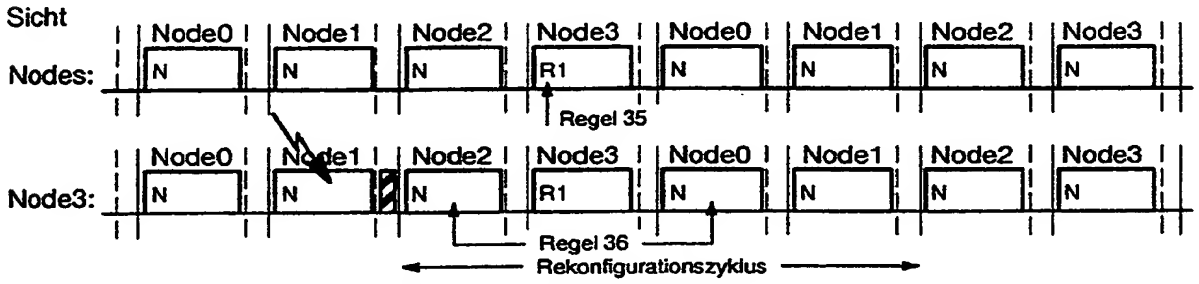


Bild 19 Stationen empfangen Frame jedoch kein VETO

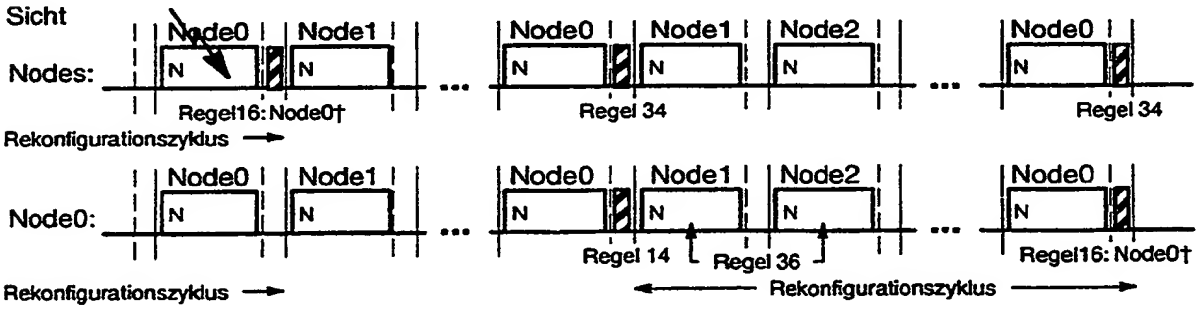


Bild 20 Eine Station (0) hat nicht bemerkt, daß sie am Ende ihres Rekonfigurationszyklus durch VETO ausgegliedert wurde

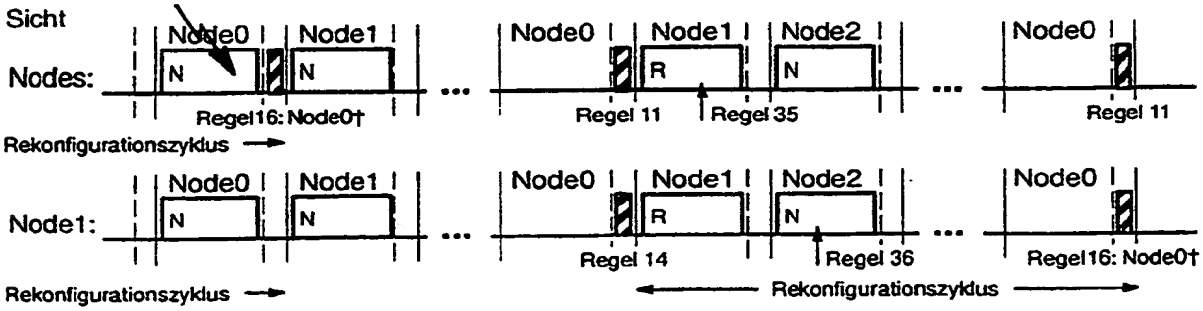


Bild 21 Eine Station (1) hat nicht bemerkt, daß eine andere Station (0) am Ende eines Rekonfigurationszyklus durch VETO ausgegliedert wurde

Nummer: DE 196 20 137 A1
Int. Cl.[6]: H 04 L 29/06
Offenlegungstag: 13. November 1997

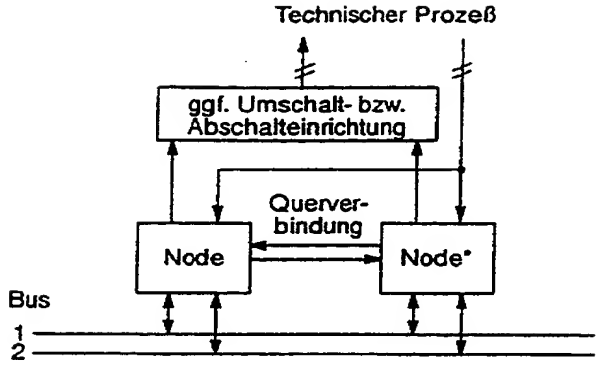


Bild 22 Zweifach redundante Station mit redundantem Kommunikationsanschluß

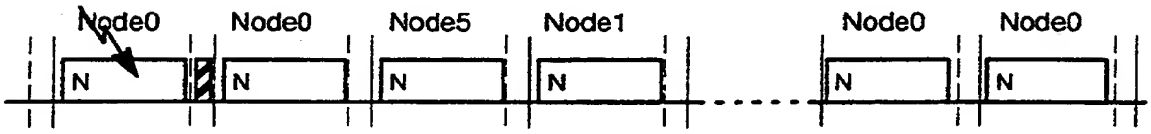


Bild 23 Störung, nachfolgende Zeitscheibe gehört der gleichen Station

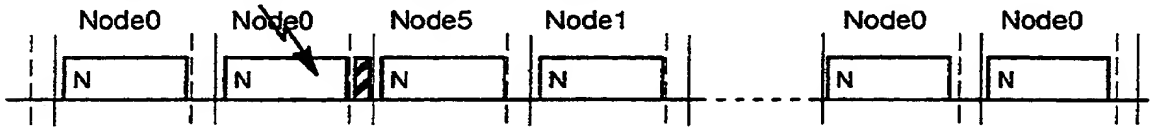


Bild 24 Störung, vorangegangene Zeitscheibe gehört der gleichen Station

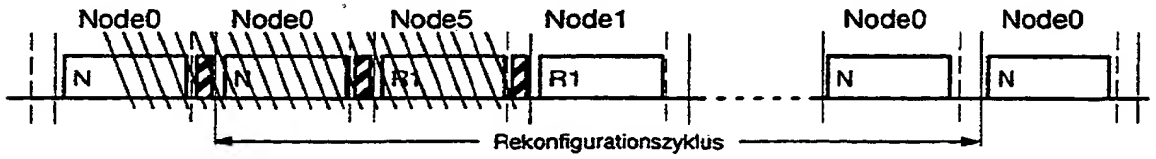
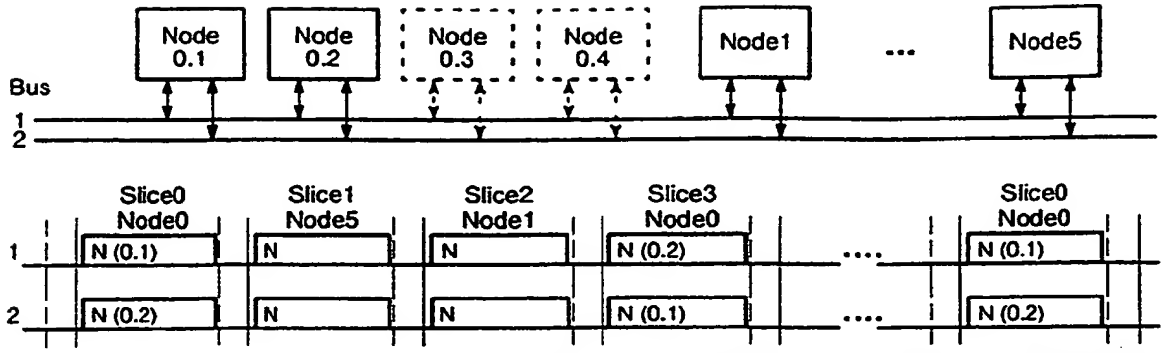
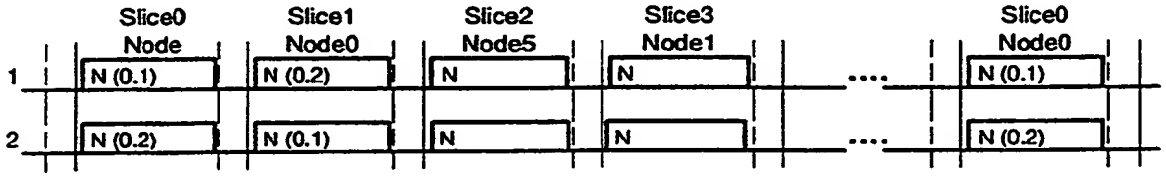


Bild 25 Anhaltende Störung, aufeinander folgende Zeitscheiben gehören einer Station

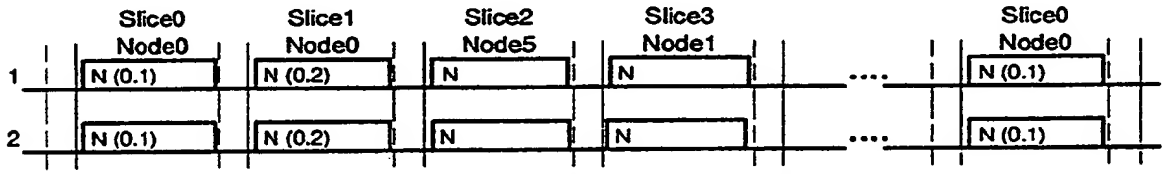
Nummer: DE 196 20 137 A1
Int. Cl.[6]: H 04 L 29/06
Offenlegungstag: 13. November 1997



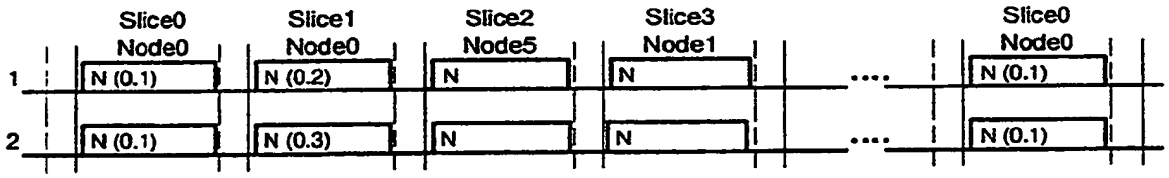
Duplex-Betrieb mit Einfachzeitscheibe, 0.1: SEND_CROSSWISE1, 0.2: SEND_CROSSWISE2



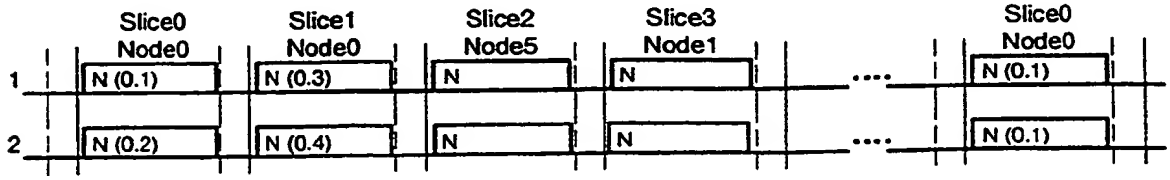
Duplex-Betrieb mit Folgezeitscheibe, 0.1: SEND_CROSSWISE1, 0.2: SEND_CROSSWISE2 (TTP-Modus)



Duplex-Betrieb mit Folgezeitscheibe, 0.1: SEND_EVEN, 0.2: SEND_ODD



TMR-Betrieb mit Folgezeitscheibe,
0.1: SEND_EVEN, 0.2: SEND_BUS1ODD, 0.3: SEND_BUS2ODD



DoppelDuplex-/Quadruplex-Betrieb mit Folgezeitscheibe,
0.1: SEND_BUS1EVEN, 0.2: SEND_BUS2EVEN, 0.3: SEND_BUS1ODD, 0.4: SEND_BUS2ODD

Bild 26 Redundante Sendemodi der Betriebsarten 2, 3, 4 und 5

Nummer: DE 196 20 137 A1
Int. Cl.[6]: H 04 L 29/06
Offenlegungstag: 13. November 1997

Zweikanaliger Betrieb mit einkanalig(defekt)er Station:

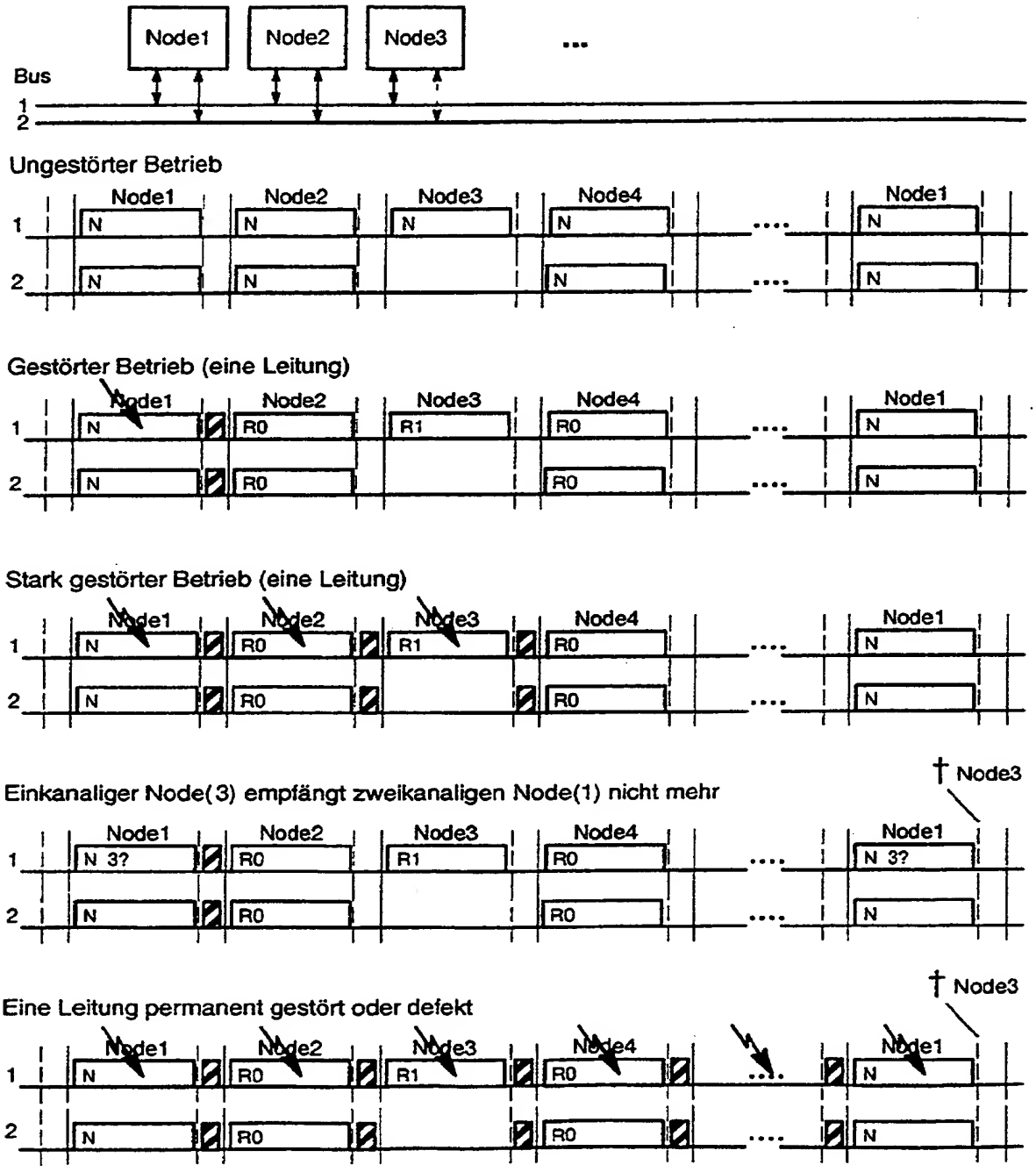


Bild 27 Protokollablauf bei gemischtem Betrieb von zweikanaligen und einkanaligen Stationen

Nummer: DE 196 20 137 A1
Int. Cl.[6]: H 04 L 29/06
Offenlegungstag: 13. November 1997

Station einkanalig defekt, zweite Station wird auf dem anderen Kanal defekt:

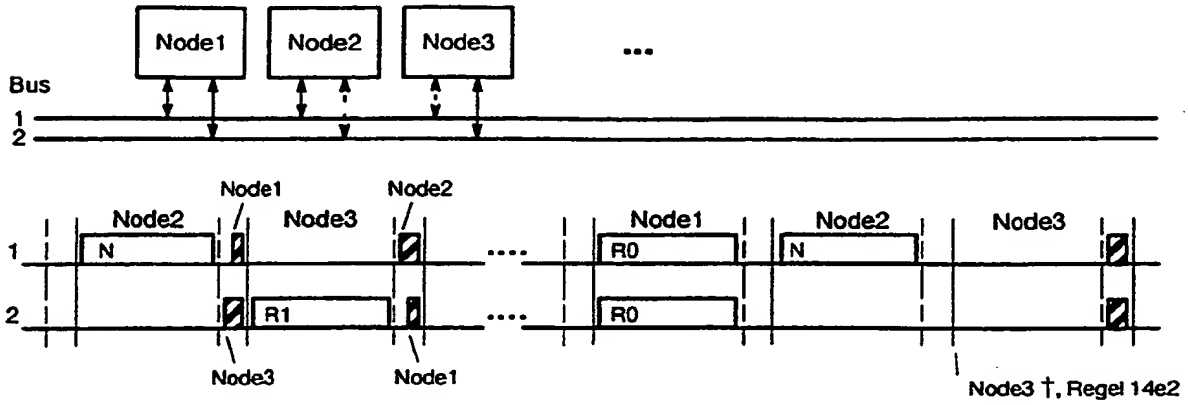


Bild 28 Ablauf bei einer einkanalig defekten Station (2), nachdem ein zweiter Kanal in einer anderen Station (3) ausfällt, der am anderen Bus angeschlossen ist.

Leitungsfehler, Trennung:

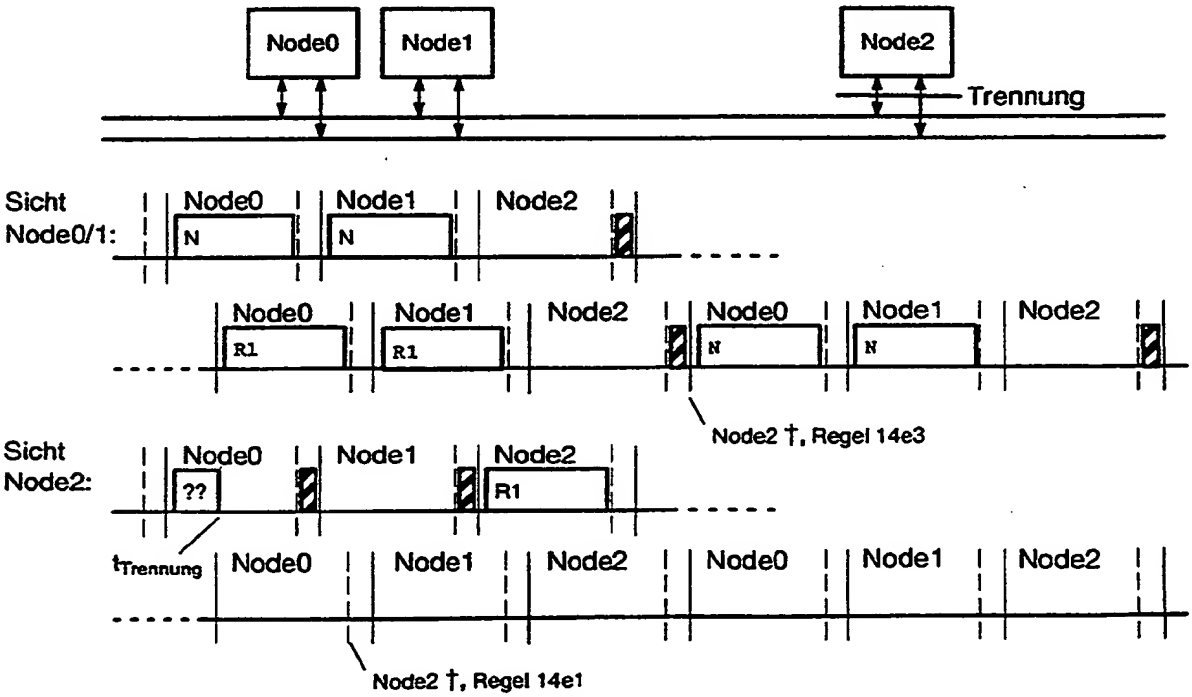


Bild 29 Ablauf des Protokolls bei totaler Abtrennung einer Station (oder Transceiver-Ausfall)

Nummer: DE 196 20 137 A1
Int. Cl.[6]: H 04 L 29/06
Offenlegungstag: 13. November 1997

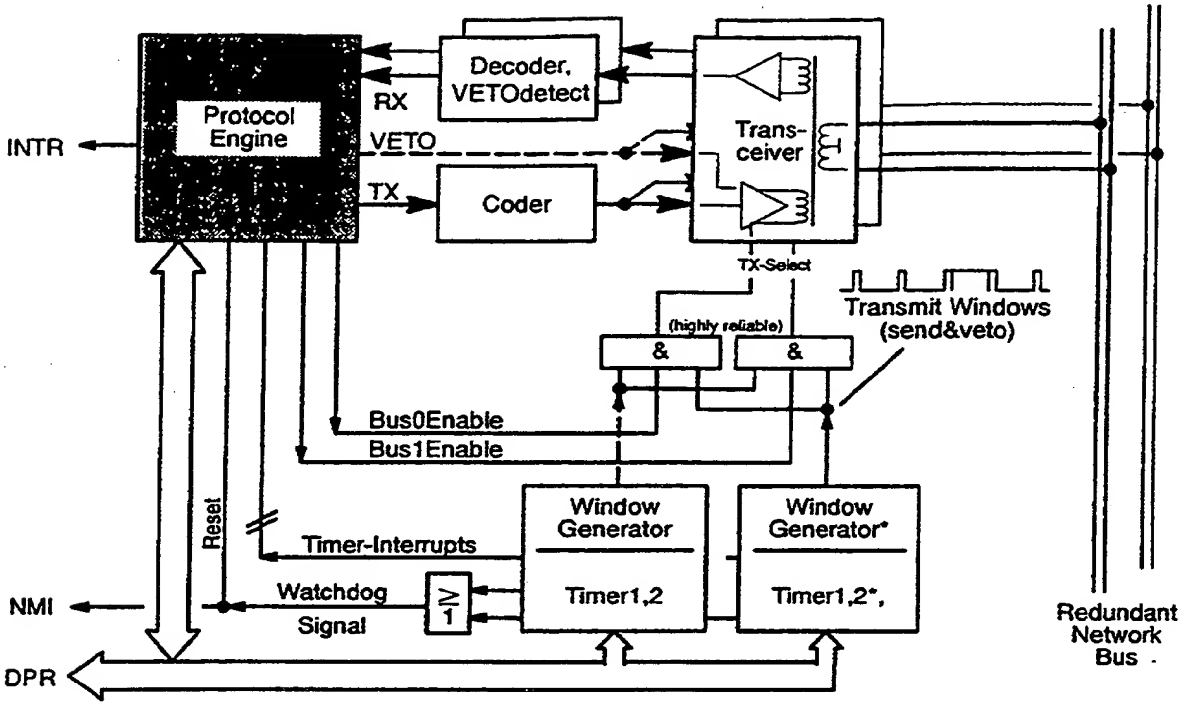


Bild 30 Möglicher Aufbau der Kommunikations-Hardware

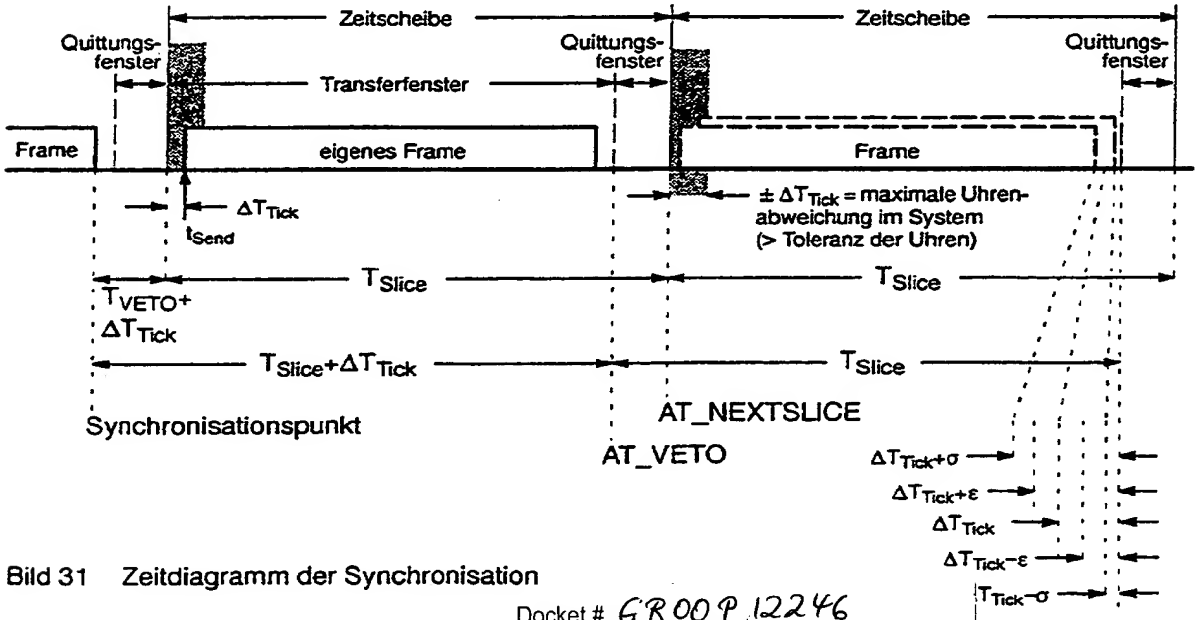


Bild 31 Zeitdiagramm der Synchronisation

Docket # GROOP 12246
Applic. # 09/883,817
Applicant: Barrenscheen et al.

Lerner and Greenberg, P.A.
Post Office Box 2480
Hollywood, FL 33022-2480
Tel: (954) 925-1100 Fax: (954) 925-1101